

EXTREME PRIVACY

WHAT IT TAKES TO DISAPPEAR

THIRD EDITION



EXTREME PRIVACY

WHAT IT TAKES TO DISAPPEAR

THIRD EDITION

MICHAEL BAZZELL

**EXTREME PRIVACY:
WHAT IT TAKES TO DISAPPEAR
THIRD EDITION**

Copyright © 2021 by Michael Bazzell

Project Editors: Ashley Martin, M.S. Williams

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. It is only offered as a printed book in order to avoid invasive digital tracking.

First Published: May 2021

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. To maintain consistency, this format is continued throughout the entire book.

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 May 1, 2021. Readers may find slight discrepancies within the methods as technology changes.

Library of Congress Control Number (LCCN): Application submitted

ISBN: 9798729419395

CONTENTS

Preface	1
Introduction.....	3
CHAPTER 1: Computers	11
CHAPTER 2: Mobile Devices	33
CHAPTER 3: Digital Life.....	97
CHAPTER 4: Home Network	177
CHAPTER 5: Ghost Addresses	211
CHAPTER 6: Nomad Residency	219
CHAPTER 7: Legal Infrastructure	231
CHAPTER 8: Vehicles.....	275
CHAPTER 9: Temporary Housing	319
CHAPTER 10: Home Purchase.....	337
CHAPTER 11: Payments, Utilities, & Services	363
CHAPTER 12: Employment.....	425
CHAPTER 13: Pets	445
CHAPTER 14: Beyond Extreme.....	455
CHAPTER 15: Damage Control	489
CHAPTER 16: Physical Privacy & Security	573
CHAPTER 17: My Successes and Failures: Jane Doe.....	587
CHAPTER 18: My Successes and Failures: Jim Doe	605
CHAPTER 19: My Successes and Failures: Mary Doe	619
CONCLUSION.....	633

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 *Open Source Intelligence Techniques* and *Extreme Privacy* are used by several government agencies as training manuals for intelligence gathering and privacy hardening. He now hosts the weekly *Privacy, Security, and OSINT Show*, and assists individual clients in achieving ultimate privacy, both proactively and as a response to an undesired situation. Details about his company's services can be found online at MichaelBazzell.com.

THIRD EDITION PREFACE

The second edition of this title was released in early 2020. Immediately after publication, I began working on this third edition. I only release a new version once I have met two specific conditions. At least one-third of the book must be new content and the remaining material must be fully relevant. This edition easily exceeds these requirements. Much of the second edition content was still applicable and only needed minor updates to reflect changes since 2020. If you have read the previous edition, you will find most of those original teachings within this book. However, I have restructured much of it to offer a better chronological order of events and included many new privacy strategies which complement the original text. To me, this feels like a whole new book. There are many overall changes which separates this edition from the others, including the following.

The first four chapters now focus solely on digital privacy and security. There is no longer an “Advanced” technology chapter later in the book. All technology methods and tutorials are presented right away, as these were the most applied techniques from the previous editions. These are also the most affordable privacy strategies which offer immediate protection and contain a large number of updates from the previous text. The methods are globally applicable and can benefit anyone who desires privacy. I believe your digital life must be properly secured before you should proceed with the remaining strategies.

This book is more extreme. The previous editions accepted the fact that most of my clients demand Apple products, iCloud accounts, overt payment methods, and easy communications. I accommodated this realization and tried to offer steps which could increase privacy while settling for inferior options. This is no longer the case. In this edition, I assume you want maximum privacy and security. I do not cut corners or pull punches. Together, we will embrace Linux on our computers; possess mobile devices without embedded Apple or Google software; create masked payment options; sanitize our past public lives; never associate our names with our homes; and rely on completely encrypted communications from open-source projects. I have no regrets from my previous writings, as I believe they served a valuable purpose at the time. Today, we must take our privacy and security to another level. After all optimal solutions are presented, I still provide alternative options for those who do not want to commit to an extreme level of privacy and security. However, I always encourage you to push your comfort level and force yourself to make the best long-term decisions.

I offer several new strategies to combat “anti-privacy” measures. Many of the techniques in the previous editions surrounding anonymous purchases, private shipping, and ghost addresses are quickly becoming blocked by companies demanding your accurate personal information. This edition presents several layers of strategies which can be customized for each specific need. Together, we will respond to various privacy invasions with a stronger defense.

I now conclude most chapters with a “Typical Client Configuration” or summary page which outlines the steps most commonly taken when a client needs the services discussed in that chapter. A valid criticism of the previous editions was that I provided too many options without clear guidance of the best path toward privacy. While I can never navigate every reader through their own unique situations, I can summarize the typical strategies for most clients. I believe this may simplify the decisions required during your own application of the content. In the previous edition, I presented numerous recommended products and services and encouraged the reader to conduct their own research to identify options most appropriate for them. In this edition, I have specified the exact products and services obtained for myself and clients. I have provided affiliate links, including many options within Amazon, throughout the book and on my website at inteltechniques.com/EP. While I see nothing about you or your order, I respect the desire to purchase anonymously through local non-Amazon services. Consider these links for research purposes, regardless of any purchase decisions.

On a personal note, this title represents my 20th published book over the past fifteen years, and a departure from writing. I will not say that I will never write another book, but I currently have no plans to publish any future editions associated with my titles about privacy, security, and OSINT. It has been a fascinating experience, but it must come to an end in order to tackle other opportunities and projects which require my full attention. I plan to continue the weekly podcast, which should be used as a resource for all future updates to these topics. I sincerely thank all of the readers who have supported my unconventional ideas and joined me during this ride. Monitor my website if you want to follow my future projects.

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 280,000 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 errors@inteltechniques.com. My team can correct anything for all future printings. The decision to restrict editing was mostly due to hard deadlines because of upcoming projects, but book piracy also played a strong role. 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 print edition, I sincerely thank you. You represent a shrinking society. If you downloaded this book from a shady site, please be careful. Many readers reported that poorly-scanned PDFs of the previous edition were infected with trackers and malicious code. Never download or open a document from any source which you do not fully trust. Please consider purchasing a legitimate copy for yourself or someone else. Sales of this book directly support the ad-free podcast which delivers updated content.

Finally, I have poured every tactic, method, and experience I have into this final edition. I hope you find something valuable here which will protect you from a growing number of digital threats. I am truly excited to introduce yet a new level of privacy and security. ~MB

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 ever be on the receiving end of this, so I took action to remove all publicly available details about me 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 client invisible to anyone searching for him or her.

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 officially disappear 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 to the internet and they want it removed. This can be very difficult as most search engines ignore these types of removal 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 I disclose some methods later in this book. A surprisingly high number of women contact me after a former lover posts pornographic videos to adult websites in 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, and 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 very vague about everything and became concerned about me knowing too much about their situations.

One of these was an individual that 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 can't vet a potential client through various 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 to which I subscribe 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, Twitter, 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 chapters 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. He or she is 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 won’t. 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 suggested extreme methods, there will be opportunities to slowly slide into privacy. **Please read the entire book before executing any strategies of your own.**

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, legal advisors, and other clients. I take my clients' privacy very 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 over a decade to create a private and secure life appropriate for my own needs, and I am still learning every day. I still make mistakes and identify ways I can improve. Our individual privacy and security playbook is never complete.

Before we jump into actionable items, I present four very important warnings. First, things will change. The first four chapters 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 subscribing to my free weekly podcast for updates.

Next, 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.

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 chapter of interest right away instead of abandoning the book during the initial chapters about technology. We all have different needs. Make this book work best for you.

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. You should not replicate anything I discuss in this book 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 make myself and my clients more private. Your scenarios will be unique from mine and your privacy plan will require modification from mine. Seek professional legal advice.**

CHAPTER ONE

COMPUTERS

This chapter represents my first major deviation from previous editions. In the past, I began with methods for establishing a ghost address because it was an easy step with an immediate feeling of gratification and success. I purposely procrastinated discussing computers in effort to appeal to those less technical than others. I now believe that establishing a secure and private computer is the absolute priority before tackling any other topics. Since you will need a computer to complete most of the techniques mentioned throughout the book, let's all make sure we are safe and secure.

I also begin here because of the abnormally high number of clients possessing compromised machines. Every week, someone contacts me because they suspect a former lover, coworker, employer, or other individual has infected their machine with malicious software configured to spy on their online activity. While some of these complaints are eventually unfounded, I have seen my share of computers sending intimate details to an unauthorized person. It can be impossible to achieve personal privacy if someone is capturing your screen every time you make a change. Therefore, we need a clean and secure computer untouched by anyone from our lives which may have bad intentions.

It is not just the former romantic partner which could be a concern. It is the companies which make the devices we trust. My first computer possessed DOS 6.22 as the operating system. There was no internet available to the masses and there was no concern of data collection by Microsoft. Today, Windows 10 pushes users to create an online account in order to access the operating system for which they have licensed. Once you load the system, Microsoft collects heaps of data about your usage and stores it indefinitely. This “telemetry” is advertised as a way to enhance your overall experience, but I find it creepy. I don't want Microsoft to collect a report about my computer habits.

Apple is no better. Some could argue that they collect even more intimate details from you as you conduct activities on your machine. They also demand an online account if you want to download their applications, and they use this as a unique data collection identifier. Did you download a podcast but only listen to the first five minutes? Apple knows this and stores it within your profile on their servers in California. Did you leave a review of an application or other Apple product? This is stored forever, associated with your account, and analyzed for potential future advertisement recommendations.

You may think I am paranoid, and maybe I am. I will let you decide if this is a concern. Consider the following types of information Apple and Microsoft collect and store on their servers about you and your devices.

- Approximate location at all times
- IP Address history
- Search history
- Typed text
- Programs downloaded and opened

This only represents the basics. If you have a microphone active on your device and did not disable the appropriate privacy settings, you could be sharing audio throughout the day. Previous editions of this book immediately focused on ways to harden Mac and Windows operating systems due to the large audiences relying on these platforms. This time, let's all become better internet citizens together. We will focus on Linux first, and only revisit best practices with Apple and Microsoft after I have exhausted all Linux considerations.

In 2018, I switched to Linux full-time, and now only use an Apple machine for production tasks (generating press-ready PDF files, recording training videos, and other tasks which are more difficult on Linux). My daily driver is a pure Debian Linux machine. However, that is not my recommendation for those new to Linux due to occasional driver and software difficulties. If you have a strong opinion of one flavor of Linux over another, I respect your choice and you likely do not need the following tutorial. If you believe Qubes OS is the most private operating system (it just may be) and you are willing to suffer through the initial learning curve, go for it! However, if you are new to Linux and desire a version which may provide an easy transition, I recommend Ubuntu. I can hear the sighs coming from tech-savvy readers who disagree, but consider my reasons.

- Ubuntu allows easy access to software packages in a graphical interface.
- Ubuntu has some of the highest compatibility with existing computers.
- Ubuntu provides easy software update options.
- Ubuntu reflects a large portion of Linux users, and online support is abundant.
- Ubuntu has fewer driver issues than other systems when adding new hardware.
- Ubuntu has removed the controversial Amazon affiliate links in previous builds.
- Ubuntu's large user base makes us all a smaller needle in the Linux haystack.

Overall, I see a higher rate of long-term Linux adoption from my clients through Ubuntu than other options. Therefore, I believe it is a great place to start. **All of the Terminal commands within this chapter, along with any updates since publication, can be found on my website at inteltechniques.com/EP for easy copy and paste.**

New Linux Computer Configuration

If you are using ANY version of Linux instead of Microsoft or Apple, you are probably achieving better privacy and security in regard to your digital life. Unlike Apple, Linux does not require an online user account in order to use core services and upgrade applications. Unlike Microsoft, Linux does not demand personal usage data. Unlike both commercial options, Linux is open-source, and the code is vetted by many professionals before each release. If you are interested in achieving extreme privacy, I hope you will consider Linux as your primary computer. The following tutorial will create a new Linux machine with slight modifications for privacy and security.

- Navigate to <https://www.ubuntu.com/download/desktop> and download the latest Long-Term Support (LTS) Desktop version. At the time of this writing, it was 20.04. By the time you read this, it may be 22.04 or 24.04. This will download a large file with an extension of ISO.
- If desired, visit <https://tutorials.ubuntu.com/tutorial/tutorial-how-to-verify-ubuntu> and verify the download based on your current operating system. This is optional, but could be important. This will confirm that the version you downloaded has not been intercepted, potentially possessing undesired software. If this sounds unnecessary to you, research the rare Linux Mint hack of 2016 when this exact scenario happened.
- Create a bootable USB device from the downloaded ISO file by installing **Balena Etcher** (www.balena.io/etcher). Launch the program, select the ISO, select your USB drive, and execute the “Flash” option.

You should now possess a USB device which is ready to install Ubuntu Linux onto a computer of your choice. If you have an old unused computer collecting dust, that is a great opportunity to try Ubuntu without committing heavily. If you only have your primary machine, you may be able to “dual-boot” both your current operating system and Ubuntu. There are numerous online guides for this. For our purposes, I will assume you are installing Ubuntu as a primary (and only) operating system directly to a machine.

I have successfully installed Ubuntu on practically every Windows and Mac machine I have possessed. If you are considering purchasing a new machine specifically for Linux, I highly recommend **System76** (system76.com). All of their laptops have the Intel Management Engine disabled. This tiny operating system within the firmware of the processor could potentially allow unrestricted, and unknown, remote access to your machine. There is much debate about the likelihood of this happening, but I welcome the paranoia. I use a System76 machine as my daily driver. This is NOT a paid endorsement, and I purchased the machine myself (through anonymous payment of course). The following will install Ubuntu Linux to your machine and harden the settings.

- Insert the Ubuntu USB device and power on the computer. If the Ubuntu install screen is not present, research the appropriate option to select a boot device for your computer. This is typically the F1, F2, F10, delete, or escape key. Pressing these immediately after powering on should present an option to boot to USB or BIOS.
- On the Welcome screen, choose “Install Ubuntu” and select your language.
- Choose “Normal Installation” and check both download options under “Other”.
- If you no longer need any data on the drive inside your computer, choose “Erase disk and install Ubuntu”. This will destroy any data present, so please be careful.
- Click “Advanced features”, select “Use LVM with the...” and choose the “Encrypt the new...” option. Click OK to proceed, then click “Install Now”.
- Enter a secure password which you can remember and is not in use elsewhere.
- If you are overwriting a used computer, consider the “Overwrite empty disk space” option. This will delete all data on the drive, and could take a long time.
- Click “Install Now”, “Continue”, choose a location, and click “Continue”
- Provide a generic name such as “Laptop”, and enter a secure password. This could be the same as the encryption password for convenience, or you could select a unique password for additional security. You will need both of these passwords every time you boot the computer. Most people make them the same password.
- Confirm your selections, allow the installation to complete, and reboot.
- Provide your password(s), then click “Skip” on the welcome screen.
- Select “No, don’t send system info”, “Next”, “Next”, and “Done”.
- If you receive a notice about updates, click “Install Now” and allow to reboot.

You now possess an Ubuntu Linux installation with full disk encryption. This prevents someone from accessing your data even if they remove your hard drive. Right away, you are very private and secure, but I always make a few modifications before introducing Ubuntu to a client. The first three Terminal commands disable Ubuntu’s crash reporting and usage statistics while the remaining steps harden your overall privacy and security. Click the nine dots (lower left) to open the “Applications” menu, scroll to “Terminal”, open it and execute the following commands. You may be prompted for your password.

- `sudo apt purge -y apport`
- `sudo apt remove -y popularity-contest`
- `sudo apt autoremove -y`
- Launch “Settings” from the Applications Menu.
- Click “Notifications” and disable both options.
- Click “Privacy”, then “File History & Trash”, and disable any options.
- Click “Diagnostics”, then change to “Never”.
- Close all “Settings” windows.

AntiVirus: This is optional, but an occasional scan for viruses is not a bad thing. Linux viruses are rare, but they do exist. You are more likely to identify viruses which target Windows machines. These could be attachments within email messages which are not a threat to your Linux installation, but should still be removed. The following commands within Terminal installs an open-source antivirus program called ClamAV.

- sudo apt update
- sudo apt install -y clamav clamav-daemon

You are now ready to update your antivirus database and conduct a scan. Type the following commands into Terminal to stop the service, update the database, and restart the service.

- sudo systemctl stop clamav-freshclam
- sudo freshclam
- sudo systemctl start clamav-freshclam

These commands download all virus definition updates and should be executed before each scan. We now have two options for a scan of our entire drive. The first scans your data and notifies you of potential viruses. However, it does not remove any files. I always execute this option first. The second command repeats the scan while deleting any infected files.

- clamscan -r -i /
- clamscan -r -i --remove=yes /

ClamAV may occasionally present a false-positive report of a virus. Do not panic. Research the file on the internet and identify the issues. If you receive reports of malicious files within email, simply delete those messages.

System Cleaner: I recommend BleachBit as my daily system cleaner. Type the following into Terminal to install the application.

- sudo apt install bleachbit

Clicking the nine dots in the lower left will present two BleachBit applications. The second icon executes the software with administrative privileges and is the option I choose. Upon first launch, click “Close” to accept default configuration. Select every option except the “Free disk space” feature. Click “Preview” to see a report of recommended cleaning. Click “Clean” to execute the process. I run this program at least once a week to remove unwanted files. **If you later install ProtonMail Bridge, be sure to deselect this option within Bleachbit.** Otherwise, your email cache will need to be rebuilt every time.

You can customize the Ubuntu interface any way desired. I like to remove unnecessary icons from the favorites bar (left) by right-clicking each and selecting “Remove from Favorites”. I then add more appropriate options as I install various programs. I also change the wallpaper and screen saver to a solid dark color. Ubuntu does not provide an easy way to do this, but the following two commands within terminal remove the background image and change the wallpaper to a neutral color.

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

Updates: It is vital to routinely update all installed applications. There are two ways to do this. You can launch the “Software Updater” program from the applications menu and accept the updates installation, or enter the following commands within Terminal. I confess I do both.

- `sudo apt update`
- `sudo apt upgrade`

Backups: Linux is private, secure, and stable, but bad things happen. Hard drives die and operating systems become corrupt. I create a backup of my home folder once per week. In the case of disaster, I can recreate my custom settings in a few minutes after installing a fresh copy of Ubuntu. Conduct the following within Ubuntu.

- Insert a USB drive into your computer
- Open the applications menu and type “backups”. Open the Backups application.
- Click “Storage Location” and choose “Local Folder”.
- Click the “Choose Folder” button, select your USB drive, and click “OK”.

You can now launch the Backups application at any time and click the “Back Up Now” button under the “Overview” tab to create a full backup of your home folder to your USB drive. As you continue to make modifications to Ubuntu, having this backup becomes more important.

You should now have a very stable, and very secure Linux operating system. The entire disk is encrypted, and you possess basic settings which will prevent most online attacks. Using Linux instead of Windows will dramatically decrease the likelihood of a virus impacting your usage. Many clients believe they cannot work in Linux because it does not offer some premium software applications. Some are surprised to discover that the vast majority of their usage is within a web browser, which they find faster in Linux than other options. Firefox is already installed and waiting. However, there is much more work to be done. Chapter Three outlines numerous services, applications, and overall habits which will help you stay private and secure while online. The basics are in place, which will ease the tutorials in later chapters.

Non-Linux Considerations

While I hope you will consider replacing your primary computer with a Linux system, I am a realistic person. Linux is not for everyone, and I do not want to exclude any readers who want to stick with Apple or Microsoft products. While the protections can never be extreme, we can still harden our Mac and Windows computers in order to afford more privacy and security. The remaining pages of this chapter are devoted to those who are not yet ready to transition to Linux.

Most of my clients are familiar with Mac products, and I believe they possess much better overall security than a Microsoft Windows system. Some clients are stuck in the Microsoft environment and insist on a Windows machine. In the next several pages, I will offer my recommendations for each of these options, and explain each step I take before handing a computer to a client. The only system I refuse to incorporate into a client's new personal digital life is a Google Chromebook. There is simply no way to achieve any privacy within that operating system.

A recurring theme is that a new device is optimal instead of trying to sanitize an existing computer. The moment you connect any Apple or Microsoft computer, tablet, or smartphone to the internet, these companies collect information associated with the Apple ID or Microsoft account (name, address, email, credit card, etc.). These companies then append this record with the unique serial number of your device, all hardware details, and the IP address of your internet connection. They now have a nice dossier on you and your hardware. This information can be seen by employees, anyone with a court order requesting these details, or potentially through a data breach.

As you continue use of these products, companies store much more of your activity such as your email contacts, wireless networks, and dozens of additional metrics. The amount of data sent to Apple and Microsoft is staggering and they can absolutely connect your recycled devices to any new alias names created during registration. If you were to format your computer and start over with a brand new name, email, and home address, Apple and Microsoft could still see the unique hardware identifiers and have the ability to connect the user accounts together.

Aside from corporate invasions into our data, I consistently meet clients which have various keyloggers, malicious software, and monitoring applications intentionally installed on their devices by stalkers, former lovers, and other adversaries. **Because of this, I always demand that high-targeted clients receive all new computer equipment.** I will begin with the most common option I see lately, which is Apple computers.

New Apple Computer Configuration

Apple macOS devices are targeted by malicious online attacks much less often than Microsoft Windows, and are considerably more secure than Windows, especially with default settings. Most clients are already familiar with the Mac environment and comfortable with the operating system. The following is my mandatory list of configurations and modifications when issuing a new Apple computer to a client.

Apple ID: When first booting a new or reformatted macOS device, you will be prompted to provide an Apple ID, or create a new Apple ID account providing your name, physical address, and email address. You have the option to bypass this requirement, but you will be prohibited from using the App Store. This eliminates many software options and disables the ability to update and patch your App Store applications. However, an Apple ID is NOT required to download and install system updates. I never attach an Apple ID to Apple computers, and I encourage my clients to do the same. If you never associate an Apple ID to your device, Apple has no easy way to store any of the activity to a profile. It also prevents accidental iCloud activation. An Apple ID is required for iOS devices, but not macOS computers. We will install all of our applications later using a package manager called Brew.

FileVault: The next step I take is to apply full-disk encryption to any new Apple device. This process is extremely easy by opening the “System Preferences” application and selecting “Security & Privacy”. Choose the “FileVault” option to see the current state of encryption on your device. By default, this is disabled. FileVault is a built-in full-disk encryption utility that uses AES-256 encryption. Enabling FileVault requires you to create a recovery key and gives you two options through which to do so. The recovery key is an emergency, 24-digit string of letters and numbers that can be used as a recovery option should you forget your password. The first option is to store the recovery key in your iCloud account, which is not advised. The second recovery option is the most secure. Your device will display the 24-digit series of letters and numbers. This code is not stored by Apple or in your iCloud account. I copy this key and paste it into my password manager, which is explained later. Alternatively, you could temporarily store it in a text file until your password manager is installed.

Once you have enabled FileVault’s full-disk encryption, your system possesses an extremely important level of security. The entire contents of your computer’s storage can only be read once your password has been entered upon initial login or after standby login. If I steal your device and attempt to extract your content via forensic process, I will only see unreadable data. By default, every computer’s hard drive is ready to give up all of the secrets until you apply full-disk encryption.

While we are in the System Preferences, let’s make a few more changes. Back in the “Privacy & Security” option under “General”, change “Require password” to “Immediately”. This will

ensure that your laptop requires a password any time you shut and open the lid. Next, choose the “Firewall” option and enable it. Note that you may need to click the padlock in the lower left in order to make changes. The firewall blocks incoming connections to the computer. This is especially important if you use public networks.

You should now have an Apple device which offers full functionality with enhanced security. Apple does not know your identity and you have not provided any personal data through the Apple stock applications. I do not recommend use of the Apple Mail, Contacts, Calendar, iCloud, Reminders, Messages, Facetime, iTunes, News, Time Machine, or Siri applications. We will use more private and secure options later. We only need the core operating system from Apple for now.

Brew: The first application I install on any new macOS operating system is a package manager called Brew. This application is very beneficial when there is a need to install programs which would usually already be present on a Linux computer. It also simplifies installation of applications which would otherwise require manual download. Brew is easily my favorite software for Mac computers. The easiest way to install Brew is to visit the website brew.sh and 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)"
```

Antivirus: There is likely no need for anti-virus applications on an Apple device, especially if you practice safe browsing habits. I never recommend commercial anti-virus products for Mac. If you insist on antivirus being present, consider ClamAV, an open-source free solution which was explained previously for Linux. Many readers scoff at my recommendation for antivirus for Mac users. Consider the following.

- The use of ClamAV on Mac and Linux computers is more about preventing the spread of bad files to Windows users instead of protecting your own machine, but viruses do exist for non-Windows systems.
- Some readers work for government or private organizations which require possession of anti-virus software on computers per internal policy.
- Some readers conduct online investigations and must defend their work in court. I was once asked under oath whether I possessed and utilized antivirus software on my work computer. I was glad my answer was not “No”. While you and I might understand the rarity of Mac and Linux viruses, the jury may not.

Brew happens to have a pre-configured version of ClamAV ready to go. After Brew is installed, type the following commands, hitting “Return” after each line, into the same Terminal application previously used. The first command disables Brew’s analytics program, which relies on Google’s services.

- brew analytics off
- brew install clamav
- sudo mkdir /usr/local/sbin
- sudo chown -R `whoami`:admin /usr/local/sbin
- brew link clamav
- cd /usr/local/etc/clamav/
- cp freshclam.conf.sample freshclam.conf
- sed -ie 's/^Example/#Example/g' freshclam.conf

These steps will install ClamAV; switch to the installation directory; make a copy of the configuration file; and then modify the configuration file to allow ClamAV to function. You are now ready to update your antivirus database and conduct a scan. Type the following commands into Terminal.

- freshclam -v
- clamscan -r -i /

The first option will download all virus definition updates, and should be executed before each scan. The second option conducts a scan of the entire computer, and will only prompt you with details of found viruses. While it may appear to be dormant, it is working, and will notify you upon completion. All of these commands must be exact. In order to assist with properly copying and pasting these commands, please use the digital versions on my website at inteltechniques.com/EP.

ClamAV may occasionally present a false-positive report of a virus. Do not panic. Research the file on the internet and identify the issues. If you receive reports of malicious files within email, simply delete those messages. Note that the above scans only SEARCH for viruses, they do not REMOVE threats. If you would like to conduct a scan and automatically remove suspicious files, you must conduct a different command. Please note this could be dangerous, and could permanently remove necessary files. I always run a scan, research the threats found, and execute the following scan ONLY if I am confident the files should be removed.

- clamscan -i -r --remove=yes /

AntiMalware: Windows users are likely familiar with the need for malware-scanning applications. This is not as necessary with macOS, but there are two malware detection applications which I highly recommend.

Task Explorer: 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. If you have installed Brew as previously explained, the following command in Terminal installs Task Explorer 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 Task Explorer. Please note that it only notifies you of issues, and does not remove them. If you have installed Brew as previously explained, the following command in Terminal installs KnockKnock to your Applications folder.

- `brew install knockknock`

Little Snitch: This software, upon first installation, is easily the most annoying application to my clients (and myself), but may provide more privacy than anything else we can install. I already mentioned how Apple constantly collects data from your machine about your usage. Little Snitch can block any outgoing data desired. It acts as an outgoing firewall. Instead of trying to block data from coming in to your machine, it stops data from being sent out. After installation and configuration instructions, I will explain a typical scenario.

- Within Terminal, execute “`brew install little-snitch`”.
- Launch the program and accept installation defaults. When prompted, click “Open Security Preferences”, then “Allow”, and close the “Security & Privacy” window. Your computer may reboot upon successful installation.
- Upon reboot, take the tour of the application. Choose “Alert Mode” and disable the “iCloud Services” option.

If you wanted to be more aggressive, you could have disabled the Apple core services option along with the iCloud Services feature. These two settings block all Apple core services, but may break many things. Since we do not want to use iCloud, disabling that feature is fine. It provides an extra layer of protection in case iCloud should become accidentally enabled. If you choose to block all Apple services, practically every stock application will refuse to connect to the internet, and you will have issues. We can always make changes later. Let's look at a few examples where Little Snitch should allow and block access to specific applications.

First, launch Firefox. You should immediately be prompted by Little Snitch asking if Firefox should be allowed to send out data to the internet. We want this to happen, so you should select the default “Forever”, then “Any connection”, and finally “Allow”. You should never be prompted about Firefox again.

Now assume that you want to add information into the stock Apple Calendar. This will only be stored on your laptop, and it should not be synchronized to an Apple server or anywhere else. When you open the calendar app, Little Snitch notifies you that the Calendar is attempting to connect to `caldav.icloud.com`. Even though you are not logged in to an iCloud account, and you have never asked Apple to sync anything for you, it sends data to their servers many times throughout every day. Little Snitch can block this. When prompted, choose “Forever”, then “Any Connection”, then “Deny”. Little Snitch will quietly block these attempts every time. If you only wish to block the domain connecting to Apple, in case you add your own calendar later, you could select the second option, “Only domain `icloud.com`”, as seen in Figure 3.01 (left).

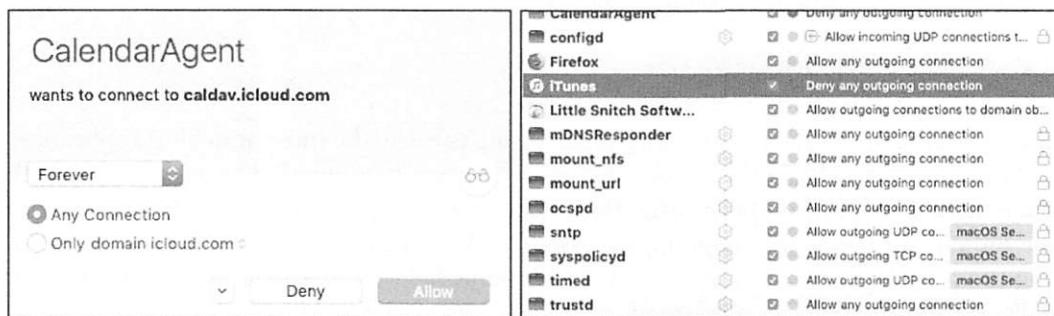


Figure 3.01: Little Snitch menus.

If you click the new menu icon in the upper right of your Desktop, you can select “Little Snitch Rules” and customize every aspect of this software. The window seen in Figure 3.01 (right) highlights my iTunes setting to block all outgoing connections. Double-clicking this entry opens the options for this configuration and allows me to change the setting or delete the rule altogether. This application requires much time for proper configuration. Once

configured, 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. Note that 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 receive nothing to promote this product.

LuLu: 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 slightly over LuLu, but the software has become quite a competitor over the past year. You only need LuLu if you do not use Little Snitch, and it may be more desirable if you are on a limited budget. Do not install both! It can be installed with the following command.

- brew install lulu

After installation, launch LuLu from the Applications folder to continue the configuration. LuLu will go through various installation steps including manual approval of its “System Extension” and “Network Filter”. Once LuLu is completely installed, 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. The “Rules” option mimics the details previously explained within Little Snitch. Both LuLu and Little Snitch have steep learning curves. However, once configured properly, they will silently protect you from eavesdropping apps.

OverSight: This product presents a small umbrella icon in the upper right menu of your Mac. By default, it monitors for any application which attempts to receive input from sound or video devices. In other words, if a program surreptitiously enabled your microphone in order to capture a conversation, OverSight would display a notification. If an application enabled your webcam, OverSight would let you know. While OverSight is free, a paid alternative made by the same company as Little Snitch is called Micro Snitch. I slightly prefer Micro Snitch over OverSight, but both offer the same features. Oversight can be installed with the following command within Terminal.

- brew install oversight

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

VirtualBox: If a client will ever need to launch a Windows machine, VirtualBox is a free virtual machine software application. It is also valuable for testing other operating systems before committing within a designated computer. I explain my usage of virtual machines within Chapter Three. If you want to install it now, the following applies.

- brew install virtualbox

Carbon Copy Cloner: This is the best full-disk backup software I have found for Mac. It allows me to create a cloned drive of my client's machine, which can be used to restore the computer back to the original state it was in during the clone. The clones can also be used as a bootable drive in case the computer operating system is completely corrupt. This is not traditional file synchronization software, which will be explained later. This program includes a free trial, but a license is required for permanent use. The following command installs Carbon Copy Cloner on your Mac.

- brew install carbon-copy-cloner

Updates: Similar to Linux, you should keep your Mac computer 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; cleanup any unnecessary cached files; and remove software no longer needed by your computer. I keep these commands digitally ready for copying and pasting within my local notes application, which is explained in Chapter Three.

- brew update
- brew upgrade
- brew cleanup -s
- brew autoremove

You should now possess a macOS computer which is stable and secure. There is still much more to be done, but you have the staples completed. In Chapter Three, we will tackle daily usage while maintaining privacy.

New Microsoft Windows Computer Configuration

Many readers may be more comfortable within the Windows environment, and choose it over Apple devices. Most businesses require Windows in order to use specific software or manage a more controlled network. Some may want a more affordable computer and never consider the overpriced Mac line of products. Regardless of your reason, Windows might be the more appropriate option for you. In my previous books, I presented privacy and security options for Windows 7, which is a much less invasive operating system than Windows 10. Windows 7 no longer receives support or scheduled security updates. Therefore, I no longer recommend Windows users continue to possess Windows 7 as an operating system. Unfortunately, we must embrace Windows 10.

By default, Windows 10 requires a Microsoft online account in order to install the operating system. The good news is that you can bypass account creation altogether by being offline. Do not choose a Wi-Fi option during setup. While offline, you will receive a prompt to “Create account later” and will be allowed to make a local account. An active Microsoft account is not required in order to receive important software updates. This eliminates the need to provide Microsoft with your name, home address, and email account. However, there is much worse news. Microsoft’s Telemetry service continuously collects the following data, plus numerous additional details, sending it to their corporate servers in Seattle.

- Typed text on 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, other trackers
- Privacy settings across 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. I find this invasive, and I will present options to disable much of the data collection. First, we must complete the installation process. If you have a new computer or are reinstalling the operating system, you will be prompted to choose “Express Settings” or “Customize Settings”. Choose the custom option which will present many choices for your new system. Disable each option presented on the screen. This will disable some of the most intrusive privacy violations such as the ability to collect keystrokes as you type and sending usage data to Microsoft.

You must now submit a username. Much like the Linux and Apple instructions, I suggest a generic account such as “Office Laptop”. Choose a strong password which you can remember. If required to provide a “Hint”, simply type the word NONE. Your computer should finish the initial boot process. After booting, enter the “Control Panel” and apply all system updates.

Similar to the Apple configuration, I want to possess full-disk data encryption. My preference for Windows 10 Pro machines is to use Microsoft’s Bitlocker. This is a proprietary encryption program for Windows which can encrypt your entire drive as well as help protect against unauthorized changes to your system such as firmware-level malware. If you have the Pro version of Windows 10, you only need to activate Bitlocker in the Control Panel by following the directions, which are similar to the Apple option. Unfortunately, if you have a Windows 10 Home version of the operating system, Bitlocker is not available to you. In this common scenario, or if you do not trust Microsoft to provide your encryption, I suggest using VeraCrypt for full-disk encryption. The following explains the entire process.

- Download VeraCrypt from www.veracrypt.fr. Execute the installer and select the “Install” option. You can accept all the default settings in the installer.
- Once VeraCrypt is installed, launch the program.
- Click System > Encrypt System Partition/Drive in the VeraCrypt window.
- You will be asked whether you want to use “Normal” or “Hidden” system encryption. The Normal option encrypts the system partition or drive normally. When you boot your computer, you’ll have to provide your encryption password to access it. No one will be able to access your files without your password. The Hidden option creates an operating system in a hidden VeraCrypt volume. You will possess both a “real” operating system, which is hidden, and a “decoy” operating system. When you boot your device, you can enter the real password to boot your hidden operating system or the password to the decoy operating system to boot it. If someone is forcing you to provide access to your encrypted drive, such as a border crossing mandate, you can provide the password to the decoy operating system. In terms of encryption, using “Normal” encryption keeps your files just as secure. A “Hidden” volume only helps if you are forced to disclose your password to someone and want to maintain plausible deniability about the existence of any other files. If you are not sure which you want, select “Normal” and continue.
- Select “Encrypt the whole drive” and choose “Single-boot”.
- Choose the encryption standard of the default setting.
- Enter a password. It is very important to choose a strong password which is unique and can be remembered. I will discuss more on this later. VeraCrypt will ask you to move your mouse randomly around inside the window. It uses these random mouse

movements to increase the strength of your encryption keys. When you have finished, click “Next”.

- The VeraCrypt wizard will force you to create a VeraCrypt Rescue Disk image before continuing. If your bootloader or other data ever gets damaged, you must boot from the rescue disk if you want to decrypt and access your files. The disk will also contain a backup image of the contents of the beginning of the drive, which will allow you to restore it if necessary. Note that you will still need to provide your password when using the rescue disk. VeraCrypt will create a rescue disk ISO image at C:\Users\NAME\Documents\VeraCrypt Rescue Disk.iso by default. You can either create a CD using this image, or simply save the ISO in case of emergency. Note that the file should be saved somewhere other than the drive which is being encrypted.
- When prompted for “wipe mode”, choose none, especially if this is a new computer.
- VeraCrypt will now verify everything is working correctly before it encrypts your drive. Click “Test” and VeraCrypt will install the VeraCrypt bootloader on your computer and restart. If Windows doesn’t start properly, you should restart your PC and press the “Esc” key on your keyboard at the VeraCrypt bootloader screen. Windows should start and ask if you want to uninstall the VeraCrypt bootloader.
- Enter your VeraCrypt encryption password when your computer boots. Sign in to your device when the normal welcome screen appears. You should see a “Pretest Completed” window. Click the “Encrypt” button to actually encrypt your device’s system drive. When the process is complete, your drive will be encrypted and you’ll have to enter your password each time you boot your computer. If you decide you want to remove the system encryption in the future, launch the VeraCrypt interface and click System > Permanently Decrypt System Partition/Drive.

After successfully encrypting your drive, you now possess a huge layer of security. If I steal your device, I cannot access your content without the password. If I remove the hard drive and connect it to a secondary forensic machine, I have no way of reading the data. This process may seem like a hassle, but the benefits are worth the effort.

Windows absolutely requires some type of anti-virus solution. I prefer the default Microsoft Defender over any commercial options. Some will say this is reckless as Microsoft Defender collects user data and submits it back to servers in Seattle. This is true, but no more invasive than the other data collection which is default with Windows 10. Basically, Microsoft already knows what you are doing. Microsoft Defender has less overhead than most commercial solutions; it is completely free; it is included with Windows 10; it automatically applies updates from Windows; and it is designed specifically for threats toward Windows 10. Therefore, I prefer it over anything else for Windows 10 users. The default settings are acceptable.

In previous books, I recommended a cleaning application called CCleaner. I no longer use this product because of some unethical practices of its owner Piriform. Some versions of CCleaner

contain Ad-ware which has been accused of collecting user metrics. My preference today is to use **BleachBit** (bleachbit.org). BleachBit is very similar to CCleaner, but can be a bit more aggressive. I select all available options with the exception of “Wipe Free Space”. Choosing this would overwrite all free space on the hard drive which is time consuming. BleachBit removes leftover internet history content, temporary files, and many other types of unwanted data. I execute this program weekly.

Next, I strongly advise users to attempt to minimize the amount of data Microsoft collects about your computer usage. I already explained a few options during the installation process, but there is much more content which needs blocked. There are many free utilities which assist with this, but I have found **O&O Shut Up 10** to be the most effective and current.

Download the latest version at <https://www.oo-software.com/en/shutup10> then install and launch the software. You will see many individual options which can be enabled or disabled. A red icon indicates that feature is disabled while green indicates enabled. The wording can be murky. In general, anything red indicates that data about that topic is being sent to Microsoft while green indicates the service is blocked.

As an example, the first option states “Sharing of handwriting data disabled”. The default option is disabled (red). Switching to green tells us that this threat is disabled, and we are protected. Some may want to play with each individual setting. Most choose a pre-determined level of privacy. In the “Actions” option at the top, you will see three categories of “Recommended”, “Recommended and somewhat recommended”, and “Apply all settings”. The first option is very safe and applies normal blocking such as disabling advertisement IDs. The second option is a bit stricter and blocks everything except automatic Windows updates, Windows Defender, and OneDrive. The last option blocks everything possible.

My preference is to select the “Recommended and somewhat recommended” option, and then enable the “Microsoft OneDrive Disabled” option. This leaves updates and Defender running. After you have made your selections, close the program and allow Windows to reboot. Open the application again to make sure your desired settings were maintained. Every time you update the Windows operating system, take a look to see if you need to re-enable your choices here. If you ever have troubles because of your level of protection, you can reverse these changes any time from within the application.

If you want to replicate the abilities of Little Snitch on Windows, check out **Glass Wire** (glasswire.com) or **Portmaster** (safing.io). Since I encourage clients to avoid Windows if possible, I do not provide a tutorial for these applications here. Neither are as robust as Little Snitch, but both offer basic protections. Apply the same methodology previously explained if you choose to test these applications.

Windows 10 Stock Application Removal

Most versions of Windows include numerous stock applications, such as “News”, “Weather”, and “Xbox games”. By default, you are not allowed to remove or uninstall these applications. They are always available to drain resources and collect data about your usage. In order to complete any tasks on these two pages, you must first set the PowerShell Execution Policy from “Restricted” to “RemoteSigned” to allow local PowerShell scripts to run. Conduct the following.

- Right-click the Windows menu icon in the bottom-left corner of your desktop.
- Select “Windows PowerShell (Admin)” and confirm execution.
- Enter “`set-executionpolicy remotesigned`” without quotes and press Enter.

The following command within this same PowerShell terminal window displays the default Microsoft applications which are included with your build.

- `Get-AppxProvisionedPackage -Online | Format-Table DisplayName, PackageName`

You can now submit a lengthy command within this elevated PowerShell window which will remove any stock Microsoft applications desired. The text on the following page removed the worst offenders from my Windows build. You may decide to submit a more or less aggressive command based on your own needs. For convenience, you can digitally copy these commands from my site online at inteltechniques.com/EP.

Once you have PowerShell launched, copy and paste the entire text on the following page from my website and submit as a single command. If you notice any applications which you do not want removed, simply eliminate those from the command before execution. You can use Notepad within Windows to modify this text as desired. Note that booting into a different user account will likely present all removed applications for that profile.

Note that any major Windows updates could replenish these applications. However, repeating the commands should remove them again. Removing these applications for one user may not impact other profiles within Windows. This method is more about removing unwanted and unnecessary applications from your instance, and does not impact much data sharing from your computer to Microsoft servers.

Whenever required, I install Windows 10 Enterprise LTSC versions of Windows for clients. This version is minimal, and does not include the Edge browser, the Microsoft Store, or the voice-activate assistant Cortana. I see these as great omissions. License keys can be purchased online as cheap as \$30, but you will need to sort through many shady vendors. The operating system can be downloaded directly from Microsoft after purchase.

```

$ProvisionedAppPackageNames = @(
    "Microsoft.3DBuilder"
    "Microsoft.BingFinance"
    "Microsoft.BingNews"
    "Microsoft.BingSports"
    "Microsoft.BingWeather"
    "Microsoft.ConnectivityStore"
    "Microsoft.Getstarted"
    "Microsoft.Messaging"
    "Microsoft.Microsoft3DViewer"
    "Microsoft.MicrosoftOfficeHub"
    "Microsoft.MicrosoftSolitaireCollection"
    "Microsoft.MicrosoftStickyNotes"
    "Microsoft.MSPaint"
    "Microsoft.Office.OneNote"
    "Microsoft.People"
    "Microsoft.Print3D"
    "Microsoft.SkypeApp"
    "Microsoft.StorePurchaseApp"
    "microsoft.windowscommunicationsapps" # Mail,Calendar
    "Microsoft.WindowsFeedbackHub"
    "Microsoft.WindowsPhone"
    "Microsoft.WindowsStore"
    "Microsoft.Xbox.TCUI"
    "Microsoft.XboxApp"
    "Microsoft.XboxGameOverlay"
    "Microsoft.XboxIdentityProvider"
    "Microsoft.XboxSpeechToTextOverlay"
    "Microsoft.ZuneMusic"
    "Microsoft.ZuneVideo"
    "Microsoft.YourPhone"
)
foreach ($ProvisionedAppName in $ProvisionedAppPackageNames) {
    Get-AppxPackage -Name $ProvisionedAppName -AllUsers | Remove-AppxPackage
    Get-AppXProvisionedPackage -Online | Where-Object DisplayName -EQ
    $ProvisionedAppName | Remove-AppxProvisionedPackage -Online
}
exit

```

Typical Client Configuration

In late 2020, I began strongly encouraging all high-risk clients to switch to Linux Ubuntu as their primary operating system. I provide most clients with a System76 Lemur Pro 14" laptop which contains all Linux modifications presented within this chapter. It possesses a hardened version of Firefox, which is explained in Chapter Three. Most clients rarely conduct any activity outside of the web browser, but all communications are also configured as desktop applications, as explained later.

This chapter emphasized the use of Linux in order to be most private and secure. However, I never want to be a Linux snob who believes computer selection is all or nothing. I was a Windows user for many years followed by five years of explicit Mac usage. Switching to Linux full-time was not easy for me. I missed the simplicity and overall visual pleasantness of macOS. There is no shame in hardening Windows or Mac to fit your current needs. However, as I write this, three of my customers running Windows have been hit with ransomware and no longer have access to their data. This probably would not have happened on a Linux or Mac computer. I avoid Windows due to privacy AND security concerns.

My bottom line is that Linux is more private and secure than Windows or macOS, and macOS is more private and secure than Windows. Some may say that Mac computers are more secure than Linux due to their "walled garden" which prevents many malicious apps from executing within the operating system. There is merit there, but the constant data collection by Mac has forced me to full-time use of Linux.

Linux is not appropriate for everyone. However, that does not excuse any reader from trying it out. Whether through installation on an old computer or within virtual machine software (explained later), I strongly encourage everyone to play around with Linux for at least a week. You may be surprised at how quickly you adapt. Linux offers a level of privacy protection which simply cannot be replicated by Windows or Mac.

Hopefully, you now possess a computer with full-disk encryption, an anti-virus solution, and an overall hardened configuration for your daily needs. These basic tutorials will likely apply to over 95% of this audience. Regardless of your choice of Mac, Windows, or Linux, you are only as secure as your online habits. Chapter Three picks up there and we have a lot to do to make ourselves secure.

Overall, this is not a digital security book; it is a privacy guide. However, I want to acknowledge that you cannot have privacy without digital security and vice versa. There are unlimited ways to configure countless mobile devices, laptops, desktops, operating systems, applications, and anything else with a digital display screen. These first four chapters present only the mandatory changes I implement during a full privacy reboot. You will likely possess numerous additional

devices that are not mentioned here. Please use the underlying messages within these chapters to make the best decisions about your own digital life configurations.

During the editorial review process for this edition, I asked technical and non-technical readers to provide input. Those without a technical background found these first four chapters overwhelming. Instead, they began with Chapter Five and read through the remainder of the book. Afterward, they concentrated on the principles within Chapters Two through Four. I believe this may be an appropriate strategy for some readers who are not tech-savvy. Please do not let the technology presented within the next three chapters steer you away from the privacy tactics within rest of the book. The next chapter is one of my favorites.

CHAPTER TWO

MOBILE DEVICES

An important step toward completely disappearing is replacing all mobile devices and accounts. 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 a client during an initial meeting that he or she 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, but while providing minimal legitimate data to the companies that benefit most from your usage.

Throughout this entire book, please remember that it is designed for the reader in an extreme situation. I will assume that your physical safety is in jeopardy, and that making any mistake is life or death for you. I will treat you like a client who is running from a homicidal former lover that is determined to kill you. I will never consider costs of products, as your safety is more valuable. I should present the bad news now. If you want extreme privacy, you need all new mobile devices. Clients often ask me if they can simply factory reset their iPhone, and my answer is always no. Consider the following argument.

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, or a rogue employee, 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. This also applies to most Microsoft and Google products.

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.

Some advocate for buying used devices in order to further confuse the systems that collect user data. I do not always 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 monitor you. We can prevent this extremely rare situation by purchasing new equipment from retail stores.

We should probably have the Apple vs. Google discussion. There are likely hardcore Android users reading this that refuse to use an Apple product. They refuse to pay the "Apple Tax" by switching over to another ecosystem. I get it. I am not an Apple fanboy, but I believe the operating system and hardware on the Apple platform is more secure and private than any official stock release by Microsoft or Google. I do not like the constant data transmissions that Apple collects and stores about your device and usage, but it is not as bad as the data collection and usage from Microsoft or stock Google products.

This is the next major deviation I take in this edition. Previously, I pushed Apple iPhone devices since they were the best easily available option. This time, let's step up our game and go the extreme route. I no longer carry an iPhone outside of my home and I encourage my clients to do the same. I would also never consider a stock Android device. The amount of location 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 these new mobile device strategies, I offer my previous methods of using Apple devices as privately and securely as possible. Choose the path best for you.

I could fill many books with the unique steps taken to replace all of my clients' hardware and online accounts, but it would likely bore the majority of the audience. Instead, I will abbreviate as much as possible, focusing only on the key elements of each phase. This is intended to be a "crash course" for the client who is ready to start over and begin a new private life, leaving all connections to previous devices and accounts behind. At the end of this chapter, I present a final basic summary of my mobile device strategy for new clients.

Let's start with the most important device to replace: your cellular telephone. If you apply only one piece of this book toward your life, I believe it should be a new anonymous mobile device with anonymous service. It is the single tracking device that we all purchase and voluntarily carry with us everywhere. We should make it as private as possible. In the next chapter, we will modify our online habits to strengthen our anonymity.

Private Android Device Configuration

My clients each receive a new telephone with new anonymous activated service. Unless my clients absolutely insist on an iPhone, I issue new devices containing custom Android builds by default. This is going to get very technical, but the final product we create will possess more privacy, security, and anonymity than anything you can buy off of a shelf. If you are not ready for this level of extreme privacy, the next section tackles an anonymous iPhone device.

The previous edition of this book presented **LineageOS** (lineageos.org) as a hardened Android custom operating system which sends no data to Google. I chose this option because it works well with hundreds of different mobile devices and compatibility seemed very important for a wider adoption. However, I no longer present this strategy. There is nothing necessarily wrong with using LineageOS, but I believe **GrapheneOS** (grapheneos.org) is a much better option. It also eliminates all data collection by Google, but introduces “full verified boot”. This feature detects modifications to any of the partitions and it will prevent reading of any changed or corrupted data. If changes are detected, such as a malicious physical attempt to compromise the device, error correction data is used to attempt to obtain the original data. This protects the device from many attacks. The authenticity and integrity of the operating system is verified upon each boot. 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 a better version. Pixel devices offer superior hardware capabilities than most Android devices. I purchased a Google Pixel 4a for \$349, paid in cash at a local BestBuy store. Used devices can be found for under \$300 on Swappa, but PayPal is required for payment. These devices are plentiful at many local retail establishments, and it is always best to pay cash for any mobile device. If you want to ensure longer support, you might consider purchasing a Pixel 5. The instructions presented here are identical for the 4a, 4a (5G), and 5. They should also work for Pixels released after publication. Always purchase the latest model which you can afford.

The following steps were modified from the GrapheneOS website at grapheneos.org/install. Always check that site before proceeding as things may have changed since this writing. I have included each step on my site at inteltechniques.com/EP for easy copy and paste. The following tutorial requires an Ubuntu Linux computer, and I used a laptop with Ubuntu 20.04 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. If you do not have a dedicated Linux computer, you can replicate the steps previously presented for installation, but choose the “Try Ubuntu” option instead of “Install Ubuntu”. This will present a temporary live Linux environment which should suffice for installation, but a dedicated Linux host is much better. Never use a virtual machine.

Phase One: Prepare Pixel Device and Linux Host

Before we can install the new software, we must prepare the phone itself. Turn on the Pixel device. Dismiss any attempts to enter a Google account.

- Swipe the menu up to launch “Settings” and click “About phone”.
- Tap “Build number” at the bottom several times until “Developer mode” is enabled.
- Click the Back” arrow and click “System”, “Advanced”, then “Developer options”.
- Enable “OEM Unlocking” and confirm the choice.
- Power off the device.

Next, we must configure software within our Linux computer. As stated previously, this can be completed within your new Linux machine or a live boot environment with a USB boot device. Full details can be found at <https://ubuntu.com/tutorials/create-a-usb-stick-on-ubuntu>. I will assume you already have a Linux laptop built from the previous chapter, but Windows and Mac options are explained at grapheneos.org/install. Conduct the following within an Ubuntu Terminal session. Note that the exact version presented here may have been updated. The tutorial steps offered at inteltechniques.com/EP will be updated as needed. Always rely on that version over any printed text here.

- `sudo apt install libarchive-tools`
- `curl -O https://dl.google.com/android/repository/platform-tools_r31.0.2-linux.zip`
- `bsdtar xvf platform-tools_r31.0.2-linux.zip`
- `export PATH="$PWD/platform-tools:$PATH"`
- `sudo apt install android-sdk-platform-tools-common`
- `sudo apt install signify-openbsd`
- `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.

Phase Two: Download & Install Graphene OS

We are now ready to download the new operating system files. First, you must navigate to grapheneos.org/releases and select your device within the “Stable Channels” section. Next, Identify the latest version number, such as “2021.05.04.01”. You will need to replace each version within the following examples (2021.05.04.01) with the latest version displayed on the website during your installation. Execute the following within Terminal.

- curl -O <https://releases.grapheneos.org/factory.pub>
- curl -O <https://releases.grapheneos.org/sunfish-factory-2021.05.04.01.zip>
- curl -O <https://releases.grapheneos.org/sunfish-factory-2021.05.04.01.zip.sig>
- signify-openbsd -Cqp factory.pub -x sunfish-factory-2021.05.04.01.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 sunfish-factory-2021.05.04.01.zip
- cd sunfish-factory-2021.05.04.01
- ./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. You may see an error about booting into a different operating system, but this is normal. Allow the phone to boot without making any selection.

Upon first boot of GrapheneOS, press “Next” until the Wi-Fi connection screen is present. Connect to Wi-Fi and complete the following tasks, with considerations for each.

- Disable location services for now, this can be set up later if needed.
- Assign a secure PIN for the screen lock.
- If desired, add your fingerprint to the screen lock function.
- Skip any restore options.

Your installation is now complete. The device itself is completely encrypted and sends no data to Google. Next, let’s harden a few settings.

Phase Three: Configuration of GrapheneOS

Once you are within the new operating system, disable OEM unlocking and developer options 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 several times until “Developer mode” is enabled.
- Click the Back arrow and click “System”, “Advanced”, then “Developer options”.
- Disable “OEM Unlocking” and confirm the choice.
- Disable “Developer options”
- Reboot the device.

Your new GrapheneOS device is very private and secure, but there is always room for improvement. There are no Google services, and Google is not receiving any data about your usage. This presents a new problem. Without Google services, there is no Google Play store which is used to obtain apps. Since we will not compromise our integrity by adding the required Google software to activate the store, we will use better options instead.

- Launch the Vanadium browser within the apps menu and navigate to f-droid.org.
- Click the “Download F-Droid” button.
- Confirm the download and click “Open” at the bottom of the screen.
- If prompted, click “Settings” and enable “Allow from source”.
- Click the back button and confirm the installation of F-Droid.
- Open the F-Droid application.
- Swipe down from the top and install any F-Droid updates available.
- If prompted, repeat enabling of “Allow from source” settings.
- 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 use the device. 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. Fortunately, updates are automatic by default and pushed to your device often. You will 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. Aurora Store is an unofficial client to Google's Play Store. You can search, download, and update apps. You can also spoof your device information, language, and region to gain access to the apps which are restricted in your country. Aurora Store does not require Google's proprietary framework. With Aurora Store, you can install most of the mobile apps mentioned throughout this book. Aurora Store can be installed through F-Droid. During installation, be sure to choose "Anonymous" mode, which prevents Google account requirements. Always attempt any app installations through F-Droid before Aurora. If an app is missing from F-Droid, rely on Aurora Store. 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.

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. In a moment, we will customize our device with communications options.

While your desired apps should install without issues, everyday function may be a problem. Since GrapheneOS does not contain any Google apps, you are likely missing some core Google software which provides services such as push notifications, location tracking, and mapping. This may sound like a huge benefit, and it very well may be, 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 simply be delayed. Some secure messaging apps, such as Signal, can deliver messages instantly through their own platform without the need for Google's push service. Traditional email applications, such as ProtonMail, may only fetch the data when the app is opened. This may be a desired feature to some. A true Google-free experience without constant 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.

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 which needs direct access to you. If you need immediate notification of incoming email and SMS text messages without launching applications, then GrapheneOS may not be for you. 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 I scare you away from GrapheneOS, let's discuss some actual experiences. If you use ProtonMail as your secure email provider, as recommended in the next chapter, you will not receive any notifications of incoming messages. You will need to open the app occasionally and check your email. If you use Signal as your secure messenger service, as recommended in the next chapter, you will receive immediate notifications of incoming text messages without the need to open the app. If you use Linphone for telephone calls, as explained later in this chapter, you will receive notification of incoming calls. Your device will ring as normal. Most other communications applications will not send notifications, and you will need to open those apps in order to see any pending messages. For most people, I believe the ability to receive incoming calls and secure message notifications through Signal is sufficient for daily use without the need for any Google 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 every day and love it. I have others who hated it. It really depends on your personality and need to be connected to everything at all times. For me, switching 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. 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 most of my clients do not use GrapheneOS. Only those with extreme situations have successfully made the switch. Today, the majority of my clients insist on iPhones. Therefore, I make them as private and secure as possible, as explained next.

Private iOS Device Configuration

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 simply demand these devices. Therefore, I am always ready to meet these expectations. I typically purchase the phones with cash at an Apple store and leave without accepting Apple's activation and setup services. Due to the COVID-19 pandemic, I have had to identify alternative solutions. When some Apple stores were closed, I was able to pay with cash at BestBuy with curbside pickup. Now that we commonly see openings of retail establishments, this may no longer be an issue. If you purchase a device online, there will always be a digital trail to your true identity. Therefore, cash in-person is always preferred.

Next, I must create new Apple accounts for each device. You can typically delay the Apple ID requirement during the first setup screen, but an account is required in order to download any apps or use the device. This brings us to our first quandary. What information should we give Apple? It would be easy to provide a fake name and address, but those days are over. Apple now requires a confirmed email address, verified physical address, and true cellular phone number during Apple ID creation from a mobile device. We can no longer supply a burner email account and Google Voice number. This is another reason I have deviated away from iOS devices. Let's tackle these issues.

I hesitate to explain any detailed process for bypassing Apple's requirement for true details, as anything I provide will become inapplicable at some point. Apple changes their requirements for Apple ID creation often. Instead of a detailed tutorial, I simply present several methods of creating an anonymous Apple ID which have worked for me in the past. Hopefully, one will work for you if needed. In a moment, I explain why this may not matter.

Mobile Device (Failure): During the registration screen on my new iPhone device, I provided a generic name, forwarding email account, hotel address, and secure password generated by my password manager (more details on all of this later). It forced me to provide a telephone number. It refused any options such as Google Voice. It demanded a true cellular telephone number and blocked any access to my device's operating system until I supplied a real number. I learned to never create an Apple ID from any Apple mobile device.

Safari Browser: Before powering on the new iPhone, I opened a web browser on a clean laptop and navigated to <https://appleid.apple.com/account>. This is where you can create a new account online. When using Firefox or Chrome browsers, the true cellular number requirement seemed strict. When connecting from Apple's browser Safari, I was allowed to provide an alias name, email address, and Google Voice number without any issues. I may have been lucky. I explain Voice Over Internet Protocol (VOIP) numbers in a moment.

Landline Number: On one occasion, Apple refused to activate an account through a web browser with a VOIP number. I chose the landline option and entered a direct-dial number associated with a guest telephone at the hotel where I was staying. The phone rang and a robot read a verification code to me. This allowed me to complete the Apple ID creation process, but I will not always have access to this phone. Apple may lock me out of my account one day. Therefore, I was sure to “update” the number to a Google Voice number later.

Windows iTunes: In 2020, I needed a new Apple ID for a client. The previous attempts were failing, so I created a Windows 10 virtual machine (explained later) and installed iTunes within it. I then attempted to create an Apple account through the Windows version of iTunes, and it allowed me to complete the process without providing a telephone number. I have no idea why this worked.

Apple Store: When desperate, I rely on the Apple store where I purchased the phone. In my experience, being connected to the free Wi-Fi at an Apple store eases many restrictions during the Apple ID creation process. On one occasion, I told the employee that I was trying to turn on my new phone, but could not provide my cellular number because I had yet to activate my new SIM card. She provided a number associated with the store and the registration process completed. She asked that I change the number in my account as soon as I activated my own cellular number. I forgot to do that.

Old MacBook: This option is a bit annoying, but it seems to work for some. If you have an older MacBook Pro laptop which originally shipped with an operating system of Yosemite or prior, you can reformat the drive and reinstall this aged OS. I held down the keys of command + option + R while powering the unit and entered the recovery partition. This allowed me to reinstall Yosemite, which does not require a telephone number to complete Apple ID registration. I only consider this if I have never associated the device with another Apple ID connected to me. This is likely the worst option for most readers.

True Number: This may seem counterintuitive, but I have provided a true cellular number to Apple while creating an Apple ID on many occasions. On the surface, this may seem reckless and unnecessary, but hear me out. In 2021, a security researcher named Douglas J. Leith from the School of Computer Science & Statistics at Trinity College in Dublin created a research paper outlining the specific data being sent from Apple and Google devices. The goal of the paper was to demonstrate that Google collects way more data than Apple, which did not surprise me. My interest lied in the research about data being sent to Apple while the device was idle. Per his research, Apple identifies and sends the telephone number assigned to every mobile device to an Apple server located at <https://gsas.apple.com/grandslam> every two to three days. Apple associates the telephone number with the device’s UDID, IMEI, SIM serial number, Apple advertising ID, and Apple security token/anisette machine identifier. This means that Apple receives and documents your telephone number and unique

hardware identifiers somewhere within their servers. If provided a court order, Apple can easily connect your specific device to its assigned telephone number. Therefore, we may not need to work so hard to keep this information secret.

The cellular provider will have their own invasive data collection and tying the two together will not expose my true identity if I practice good mobile device hygiene. In a moment, I explain my preferred pre-paid cellular provider (Mint Mobile), which can be purchased without providing a true name. The SIM can be anonymously activated through an app over Wi-Fi within the Apple store. I prefer to use public Wi-Fi without a VPN in order to avoid fraud triggers from the cellular provider. If I buy a phone with cash at the store and activate a SIM in an alias name via Wi-Fi, I see little harm in sharing this number with Apple. It appears much more legitimate than burner VOIP accounts and will be much less prone to lockouts. This method has never failed me and may be most stable option for many readers.

Throughout 2021, I was asked to purchase and activate numerous Apple iOS mobile devices for my clients. The following is a summary of the required steps if you do not have another device available for cellular activation, and I explain more about my chosen cellular service provider in a moment.

- Purchase a device in-store with cash. Explain that you need to download an app to activate your new SIM in order to receive a cellular number (required by Apple ID). Ask for a demo unit which allows download of apps. The store should be able to provide a demo iPhone which does not have app downloads restricted. Download the Mint Mobile app, insert your new trial SIM (explained soon) and activate it. Note the new telephone number.
- Create a new Apple ID from your new purchased device. When prompted, provide the number issued by Mint Mobile. Confirm the verification text sent to the demo.
- Remove the SIM from the demo unit and place it in your new phone.
- Download the Mint Mobile app on your new device; delete the app from the demo; and change your Mint password from the new device.

Note that I always possess a GrapheneOS or other Android mobile device for the purpose of activating new SIM cards. This eliminates the hassle of downloading the Mint app at the Apple store on behalf of my clients, and ensures I have a cellular number ready for Apple ID creation. There are benefits to connecting your new true number to your Apple ID. If you should break the device or become locked out of your Apple account, you have an ability to confirm authorization through the telephone number. You can also use this number as part of a Two-Factor Authentication routine within the Apple network. I explain more on this in the next chapter. If you possess a new cellular data account in an anonymous name, as explained soon, I see very minimal risk in attaching your provided number to your Apple ID. It may prevent lockouts and a requirement to create new accounts.

Once you have a username and password for Apple ID, it should work for any device. I always add some type of secondary VOIP telephone number to every Apple ID I create in order to avoid future lockouts. I present many options for this in just a moment. For extreme privacy, this device should never be configured from your home. Most phones have location services, Wi-Fi, Bluetooth, and cellular connectivity enabled by default. This could expose your account and associate it with your residence. I will explain in a moment how I isolate my phone from my home.

If you plan to purchase apps, obtain a prepaid iTunes gift card with cash from a grocery store. Never provide Apple with a credit or debit card number. 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 second generation iPhone SE. This device has plenty of power and is affordable at \$399. 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 present more thoughts on this on the next page. In previous editions, I recommended the first generation iPhone SE. While I still have a few, including one that sees daily usage on international travel, these are difficult to find today. Furthermore, this outdated device will soon stop receiving security updates and patches. I no longer recommend people seek this model.

Regardless of the model, I immediately disable all iCloud services within the device. 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. You can access these settings from the iOS "Settings" app > "Apple Account" > "iCloud". You should have the option to completely sign out of iCloud and the final result should display "Off" within this menu. Hopefully, you were never signed in.

Some may question my distrust of iCloud. A more appropriate claim would be that I don't trust any cloud storage services 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. I will discuss solutions in a moment. Most of my clients are highly targeted due to their fame, so I insist on completely disabling iCloud or any other storage solution.

The next priority is managing the privacy settings of each application. You must give your applications reasonable access to only the settings they need in order to perform their desired task. Navigate to "Settings" > "Privacy" and conduct the following modifications.

- Location Services: Turn to the “Off” position. Change this only when in need of a mapping service. Disable individual permissions if you plan to use this feature.
- Contacts: Limit the applications which should have access to your contacts. Services such as communications apps must see your contacts in order to connect you to other people, but other apps should not have access.
- Calendars: If you do not use the stock Calendar app (I do not), then this can be disabled within every application presented.
- Photos: If you never share photos through any apps, it is safe to disable this within every program. It can be enabled if you change your mind.
- Microphone: This should be limited to the applications which truly need access to the microphone to perform their intended function, such as voice messaging applications.
- Camera: This should be limited to the applications that truly need access to the camera to perform their intended function, such as messaging applications which you wish to share photos and videos from your camera. Disable any app which should not have the authority to access your camera.
- Health: Disable completely.
- Homekit: Disable completely.
- Motion & Fitness: Disable completely.
- Siri: Disable and delete all Siri options and data at the following locations:
“Settings” > “Privacy” > “Analytics & Improvement” > “Improve Siri & Dictation”
“Settings” > “Siri & Search” > “Siri History” > “Delete Siri & Dictation History”

Under “Settings” > “Touch ID & Passcode”, select “Change Passcode”. The default option is a maximum of six numbers, which I believe is insecure. Select “Passcode Options” and then “Custom Numeric Code”. This will allow you to set a longer passcode. I recommend a minimum of twelve numbers. 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.
- 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 would never consider using this. Although Apple does not store your image, it has been proven vulnerable using images of faces to unlock the device.

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 computer 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 (a tutorial is in the next chapter). 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.

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.

Cellular Service

Now that your device is configured, your privacy settings are tweaked, and your operating system is more secure, you will need cellular service. In major U.S. metropolitan areas, I use Mint Mobile as the provider. Mint is a T-Mobile reseller, and only offers 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 SIM card. I only need the data, as my clients will never use their real T-Mobile issued number for calls or texts.

You can obtain 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 (more on that later), but this may be overkill for your needs. If you only need one or two devices activated, I recommend purchasing the Mint Mobile Starter Pack online from Amazon (amzn.to/3d2qXyG) or in-store from BestBuy. The following are two recommended strategies.

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 Mint Mobile credit. I have been able to purchase dozens at a time.

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. I explain many Amazon considerations later in the book.

After you possess a Mint Mobile SIM card, install the Mint Mobile app on the device you recently configured. This should be done away from your home. If possible, use public Wi-Fi at the place of purchase, as I previously explained. Insert the SIM card and activate the card through the app. This provides you one week of free service to ensure the coverage is acceptable to your needs. It is using T-Mobile service, and I have found the coverage much better than years past. Once you are convinced that Mint Mobile will work for you, select a package within the app. I use very little data, so the 3GB LTE (unlimited at slower speeds) is plenty for my needs. You can prepay for three, six, or twelve months. The longer you commit, the cheaper the price. The lowest package can be purchased for \$15 monthly at the yearly commitment. I later explain anonymous payment options. Some readers report the ability to activate “3 month” Mint Mobile prepaid SIM cards from retail stores through the Mint website without a requirement to download their application. This can be helpful for new iOS devices.

Existing Devices and Service

For extreme privacy, you truly need to eliminate any Apple or Android device which was ever associated with your true identity. Apple and Google hold on to this data forever. They can determine when you log into a new anonymous account within the same hardware. However, privacy is not all black and white. There are grey areas. Many readers have informed me that they cannot afford new hardware and are stuck within cellular service contracts which cannot be terminated. This page offers some considerations for these scenarios.

iOS: If you want to use your current mobile device but want to reclaim a bit of privacy, conduct a hard reset. This erases everything on the device and allows you to create a new Apple ID. Navigate to “Settings” > “General” > “Reset” > “Erase All Content and Settings”. This deletes everything, so make sure you have backed up any important content such as photos, videos, and documents. Apple will be able to associate your serial number with both your old and new accounts, but future data collection will be applied only to the new profile.

Android: The steps to reset Android devices vary by version and manufacturer. Many allow you to reset the device from the “Settings” menu within Android. Tap “System” > “Advanced” > “Reset options” > “Erase all data (factory reset)” > “Reset phone”. If required, enter your PIN, pattern, or password. Upon reboot, you should be requested to provide Google account credentials. Consider skipping this option and applying the privacy principles surrounding F-Droid and the Aurora Store as previously explained.

Service: If you cannot initiate new cellular service, consider sanitizing the account you have. Most cellular providers supply registered user details for use with caller identification services. The name on your account is likely shared with numerous third parties. You can control some of this. Sign in to your account and find your profile. Modify the name if allowed. The name on this profile is typically what is shared with third parties and appears on caller ID screens when placing a call. The following displays the current instructions for the popular U.S. providers. An online search should identify the proper steps for your provider.

AT&T: Profile > Account users > User

Sprint: My Account > Profile & Settings > Limits & Permissions > Change Caller ID name

T-Mobile: (Must call customer service)

Verizon: Account > Add-ons > See All > Share Name ID > Product details > Manage

Recycling devices and service always leaves a trail, but these options are better than doing nothing at all. There is no room for elitism in this game, and any steps you take can provide numerous layers of protection as you navigate the complicated world of privacy and security.

Voice Over Internet Protocol (VOIP) Considerations

Now that you have a new device with a new data plan, you are set. Install only the apps you need, and proceed with private use. Since you should never use the number provided from your cellular company, you will need a way to make and receive standard telephone calls and text messages. If you elected to take the GrapheneOS route, you will rely on an application called **Linphone** (linphone.org) for VOIP telephone service. First, let's understand the reasons we should not use our true cellular number.

- When you make calls and send texts 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 communication 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 cell towers. I can abuse court orders to obtain these details or hire a criminal to breach your account.
- Cellular telephone numbers are prone to SIM-swapping attacks. If I know your primary number, I can take over your account through various attacks and become the new owner of the number. I can portray you and receive communication meant for you.
- 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. Lately, services such as Twitter and LinkedIn are the bigger concern. 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. Giving out VOIP numbers eliminates much of the concern of this threat.

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 a service called Twilio for telephone calls and SMS text. Afterward, I provide a much easier experience through a service called Telnix. Both have advantages and disadvantages. Twilio is our most robust option, so let's start there.

Linphone/Twilio VOIP Configuration

My goal within the next pages is to create our own VOIP product which allows us to make and receive telephone calls on any device we desire at minimal cost. Furthermore, the numbers will be in our control. We 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 without notice. It is probable that you will encounter slight variations compared to my tutorial during configuration. Focus on the overall methods instead of exact steps. The following explains every step I took in order to create my own VOIP solution with Twilio. After, I present another option which may be more appropriate for some readers. Please read the entire chapter before making any decisions.

The first step is to create a new account at <https://www.twilio.com/referral/9FGpxr>. This is my referral link which gives you \$15 of free testing credits and \$10 of free full usage credits. I see absolutely nothing about you or your usage. You must provide a name, email address, and phone number to Twilio as part of this process. Twilio possesses strong fraud mechanisms in order to suspend accounts which seem suspicious. During the first tests of this strategy, my accounts were immediately suspended. I had provided a vague name, burner email address, and Google Voice number while connected to a VPN. This triggered the account suspension and I was asked to respond to a support email explaining how I would be using Twilio.

This began communication with two Twilio support personnel. While talking with customer service, I was advised that the VPN IP address was most likely the reason for the suspension. After providing a business name, “better” email address, and explanation that I would be using the product for individual VOIP solutions, my account was reinstated. If you get caught within this dragnet, I encourage you to let them know you are following the protocol in this book to establish “VOIP through Linphone”. I think you will find your account restrictions lifted within an hour. Twilio may push for a real phone number, but I have never provided anything besides a Google Voice number (explained later). My advice is to provide a unique name, non-burner email address (preferably your own domain), and Google Voice number during registration. If Twilio demands a copy of government ID, push back. I was able to activate two accounts without ID after initial suspension. Overall, they just want paid users who do not abuse their networks.

I will now assume that you have a Twilio account created with a strong password using the previous link. The free credits allow us to test many features of the service, but a \$20 deposit will be required before our account is fully usable. Clicking on the upper left “down arrow” should allow you to create a new project. Choose this and provide a name for it. I called mine “VOIP”. This will likely require you to confirm a telephone number to “prove you are human”. Fortunately, they accept VOIP numbers here, and I provided a Google Voice number. After confirming the number, answer the questions presented about your desired

usage. The answers here have no impact on your account. Once you have your new project created, you should see the new \$15 test balance. It is now time to configure our VOIP telephone number. First, determine the locality of the Twilio server closest to you, based on the following configurations. I will be using the “East Coast” U.S. option, so my example server will be [phone number].sip.us1.twilio.com. The most stable option in the U.S is “us1”.

- North America Virginia: [phone number].sip.us1.twilio.com
- North America Oregon: [phone number].sip.us2.twilio.com
- Europe Dublin: [phone number].sip.ie1.twilio.com
- Europe Frankfurt: [phone number].sip.de1.twilio.com
- South America Sao Paulo: [phone number].sip.br-1.twilio.com
- Asia Pacific Singapore: [phone number].sip.sg1.twilio.com
- Asia Pacific Tokyo: [phone number].sip.jp1.twilio.com
- Asia Pacific Sydney: [phone number].sip.au1.twilio.com

Please note that I have supplied all of the required Twilio code text on my website at inteltechniques.com/EP in order to allow easy copy and paste. If the following menu items have changed, look for the “Legacy” menu or identify any new labels. Twilio changes their menu options often without warning or updated documentation.

- Within the Twilio Dashboard, click “Get a Trial Number”. Either accept the generated number or use the search feature to find a number within your desired area code. This will deduct \$1 from your trial balance. My demo number is “2025551212”.
- If this option is not present, click the “All Products and Services” icon in the upper left menu, then “Phone Numbers”, then “Buy a Number”. Enter your desired area code and “Search” for a suitable number. Click “Buy” next to the desired number.
- Click the “All Products and Services” icon in the upper left menu.
- Choose the “Programmable Voice” menu option.
- Click the “SIP Domains” option and click the “+” to create a new domain.
- Enter the assigned telephone number as the “Friendly Name”, such as “2025551212”.
- Enter the assigned telephone number as the “SIP URI”, such as “2025551212”.
- Under “Voice Authentication”, click the “+” next to “Credential List”.
- Enter a “Friendly” name of your number, such as “2025551212”.
- Enter a “Username” of your number, such as “2025551212”.
- Enter a secure password and click “Create”.
- Under “SIP Registration”, click the “Disabled” button to enable it.
- In the “Credentials List” drop-down, choose your telephone number and click “Save”.
- Click the “All Products and Services” icon in the upper left menu.

- Click “TwiML Bins” and select “Create a New TwiML Bin”.
- Provide a “Friendly” name of “incomingvoice”.
- Place the following text in the TwiML box. Replace “2025551212” with your number.

```
<?xml version="1.0" encoding="UTF-8"?>
<Response>
<Dial answerOnBridge="true">
<Sip>2025551212@2025551212.sip.us1.twilio.com</Sip>
</Dial>
</Response>
```
- Click “Create” and “Save”.
- Click the “All Products and Services” icon in the upper left menu.
- Click the “Phone Numbers” menu and click your telephone number.
- Under “Voice & Fax”, then “A Call Comes In”, choose “TwiML Bin”.
- Select “incomingvoice” in the drop-down menu and click “Save”.
- Click the “All Products and Services” icon in the upper left menu.
- Click “TwiML Bins” and click the plus sign to create a new bin.
- Provide a “Friendly” name of “outgoingvoice”.
- Place the following text in the TwiML box, copied from my site.

```
<?xml version="1.0" encoding="UTF-8"?>
<Response>
<Dial answerOnBridge="true" callerId=
"{{#e164}}{{From}}{{/e164}}">{{#e164}}{{To}}{{/e164}}</Dial>
</Response>
```
- Click “Create” and “Save”.
- Click the “All Products and Services” icon in the upper left menu.
- Click “Programmable Voice” and click “SIP Domains”.
- Select your domain.
- Under “Call Control Configuration” then “A Call Comes In”, change “Webhook” to “TwiML Bin” and select “outgoingvoice” in the drop-down menu.
- Click “Save”.

You now have a SIP domain and credentials created which allow you to associate your Twilio account with VOIP software called **Linphone** (linphone.org). Navigate to this website and download the desired application for your environment. I downloaded the Linux, macOS, Android, and iOS apps to my laptops and mobile devices. I downloaded it to my GrapheneOS device through F-Droid as previously explained. The following configuration steps should apply to all Linphone applications, but you may see minor variations across platforms. You will need to repeat each step on every device which you want to use for VOIP calling. I will explain the process of configuring Linphone on a laptop in the next chapter.

- If prompted upon launch of Linphone, choose “Account Assistant”.
- Click the “Use a SIP Account”.
- Enter a “Username” of your number, such as “2025551212”.
- Enter a “Display Name” of your telephone number, such as “2025551212”.
- Enter a “SIP Domain” of your full domain including your username and the closest server location as previously explained. I used 2025551212.sip.us1.twilio.com. Replace “2025551212” with your own number and “us1” with your server.
- Enter the “Password” you previously created for the credential account.
- Change the “Transport” to “TLS”.

Click the confirmations until you return to the main application. You can now click the upper left corner in order to select your new account, or choose between multiple accounts if you add more. You should see a green or grey light next to the account if the connection from Linphone to Twilio is successful. We can now make our first test call.

- Confirm that your Twilio account is selected within the Linphone application.
- In the search field at the top, input any known telephone number.
- Click the “phone” button to initiate a call.

You should receive an automated message thanking you for using your demo account. This confirms that we can place calls to Twilio’s servers, but we are far from unlimited usage to real numbers. We are now ready to attempt a stricter test call. You still cannot call any real number, but you should be able to place a call to any “Verified” number. If you provided a Google Voice number during account creation, that number is automatically verified. If you did not, complete the following to add a verified number for testing.

- Click the “All Products and Services” icon in the upper left menu.
- Click the “Phone Numbers” option and click “Verified Caller IDs”.
- Add a new number which can be accessed.
- Confirm whether you prefer a call or text and verify the call or text to add the number.

Return to your Linphone application and attempt a call to the number which you have verified with Twilio. For me, it was my Google Voice number. After a brief message about the trial account, the call should go through. If you can complete a test call to your own number, your configuration is complete. You are now restricted to only calling verified numbers. I have seen this fail with some VOIP numbers. If this happens to you, do not be alarmed. As long as you receive a confirmed test call message from Twilio, your configuration is complete. If you would like to remove all restrictions to make and receive calls to and from any number, you must “Upgrade” the account. The following should be conducted within the Twilio portal.

- Return to the Dashboard in the upper left menu.
- Click the “upgrade” link and provide all requested billing details.
- Provide any credit, debit, or registered prepaid card.
- Apply \$20 to the account.

You should now have an unrestricted Twilio account which should be fully functional for voice calls. Please do not upgrade the account until you know your test calls are going through. You should also have a fully functional VOIP application which can facilitate calls. Linphone can be used to place a call at any time from any device. Replicate your Linphone settings on as many mobile and desktop environments as you desire. Furthermore, you can add as many numbers as you wish by repeating this process.

Incoming calls will “ring” your mobile device or desktop as long as the Linphone application is open and your status is “green”. Before you create dozens of new numbers, let’s discuss the costs. Each Twilio number withdraws \$1.00 every month from your balance. If you followed these steps, you are funded for almost three years of usage of the initial phone number. Incoming and outgoing calls cost \$0.004 per minute. During all of my testing for this tutorial so far, I spent \$1.21. There are several huge benefits with this strategy, as outlined below.

- You can now make and receive telephone calls through practically any device. Windows, Mac, Linux, Android, and iOS are all supported through Linphone apps.
- You have more control over your number(s). You are not at the mercy of Google, and their data collection, in order to process calls.
- You can add as many numbers as desired as long as you have the funds to support them. I have five numbers through Twilio and I can access all of them through every device I own. My annual cost for this, including my usage, is about \$70. Twilio does not know my real name and only possesses a custom domain email address and Google Voice number in association to my account.
- You can port a number into Twilio. If you plan to cancel a cell phone or VOIP number, you can port it into Twilio and still have access through Linphone.
- This process works well with custom Android ROMs, such as GrapheneOS, as previously explained.
- You can call international numbers (at increased costs). Most VOIP providers such as Google, Twilio, and others restrict calling to nearby countries. You can enable any country in Twilio by navigating to Programmable Voice > Calls > Geo Permissions.

Please think of this VOIP strategy as being similar to landline service. Linphone has no embedded voicemail or SMS text message capabilities and is only for voice calls. If you desire the ability to receive SMS text messages associated with this new Twilio number, conduct the following steps, or consider the forwarding strategy explained in a moment.

- Click the “All Products and Services” icon in the upper left menu.
- Click the “TwiML Bins” option and click the red plus to add a new bin.
- Provide a name of “incomingsms”.
- Insert “<Response></Response>” within the TwiML field and click “Save”.
- Click the “All Products and Services” icon in the upper left menu.
- Click “Phone Numbers” and select your number.
- Under “Messaging”, and “A Message Comes In”, choose “TwiML Bin”.
- Choose “incomingsms” in the field to the right and click “Save”.

Any incoming text messages to this number can now be read in the “Programmable Messaging” menu option in your Twilio account. SMS text messages cannot be pushed to, or sent from, your Linphone application using this VOIP strategy. While it is possible to implement this feature, it requires creation of a dedicated app and hosting your own web server, which exceeds the scope of this book. If you want to forward any incoming SMS text messages to another number, such as Google Voice or MySudo, replace “<Response></Response>” from this tutorial with the text below. Replace 2125551212 with any number which you want to receive the text messages intended for your new Twilio number.

```
<Response>
<Message to='+12125551212'>{{From}}: {{Body}}</Message>
</Response>
```

Advanced users may want to instantly forward any incoming SMS text messages to an email address. This is what I prefer, but it requires an online web server. A shared host and any custom domain, as explained later, will suffice. Create a text file called twilio.php with the following content. Change “your@email.com” to the address where you want to receive notifications. Change “@yourdomain.com” to your actual domain name. Upload this file to your web host. This text is also available on my site for easy copy and paste.

```
<?php
$to = "your@email.com";
$subject = "Text Message from {$REQUEST['From']} to {$REQUEST['To']}";
$message = "{$REQUEST['Body']}";
$headers = "From: twilio@yourdomain.com";
mail($to, $subject, $message, $headers);
```

Navigate to your Twilio dashboard and conduct the following.

- Click the “All Products and Services” icon in the upper left menu.
- Click “Phone Numbers” and select your desired number.

- Under “Messaging” and “A Message Comes In”, change each entry to “Webhook”.
- Provide the full address of the PHP file you previously created within both fields. This may be similar to <https://yourdomain.com/twilio.php>.

Test your new SMS option from another number. Any incoming SMS messages to your Twilio number should now be forwarded to your email. The subject will appear as “Text Message from 2125551212 to 6185551212” and the body will contain the message sent. I prefer this option because it does not require another telephone number, such as Google Voice, in order to receive messages. When I give my car dealer this Twilio number during a maintenance visit, I receive an email when they send a text notifying me my vehicle is ready.

If you want to send SMS text messages from your Twilio number, you have two options. There is a “Try it out” feature within your Twilio dashboard, but I find this process cumbersome and it relies on you to be constantly logged into Twilio. Instead, consider a “Quick Deploy” option provided by Twilio. First, navigate to the following website.

<https://www.twilio.com/code-exchange/browser-based-sms-notifications>

Next, confirm that the “Account name” is the VOIP project which you created for this process. If you have more than one number, select the appropriate option. Finally, create a passcode which prevents random people from finding your project and sending messages. This should be a fairly secure passcode, but should also be rememberable. When finished, click “Deploy my application”. You will be presented a static URL similar to the following.

<https://sms-notifications-6431-bf4jg3.twilio.io/index.html>

Visiting this page presents a form which allows unlimited outgoing SMS text messages from your new Twilio number. Enter one or more target numbers; apply your application passcode; and write your message. Be sure to bookmark this page within your desktop and mobile browsers in order to access it easily. If you want to send a response to a received message, you can open your new Twilio page and send it from there. To be fair, I do not do this. It is simply too much effort. However, I know that many readers want a complete SMS option directly within Twilio. I explain my own usage of secure text messages later.

Next, consider voicemail. Some may prefer to have no option to leave a voice message. The instructions up to this point will either ring your Linphone application for 30 seconds and then hang up, or simply terminate the call right away if Linphone is not open and connected. I prefer this for some numbers, as I do not want the caller to be able to record a message. However, we can enable voicemail, tell Twilio to record the message, save it to their servers, and email us a link of the recording. Conduct the following within the Twilio Dashboard.

- Click the “All Products and Services” icon in the upper left menu.
- Click “TwiML Bins” and select “incomingvoice”.
- Replace the current text with the following.


```
<?xml version="1.0" encoding="UTF-8"?>
<Response>
<Dial answerOnBridge="true" timeout="30"
action="http://twimlets.com/voicemail?Email=your@emailhere.com">
<Sip>2125551212@2125551212.sip.us1.twilio.com</Sip>
</Dial>
</Response>
```
- Replace “your@emailhere.com” with your desired email address.
- Replace “2125551212” with your own SIP Domain name.
- Replace “us1” with your own server location if necessary.
- Click “Save” and test the service.

If your Linphone application is open and connected, an incoming call should ring for 30 seconds. If you do not pick up the call in that time, the voicemail system presents a generic greeting and allows the caller to record a message. If Linphone is closed or not connected to Twilio, the greeting is presented right away. If a caller leaves a voicemail, you will receive an email at the address provided which includes a link to hear the recorded mp3 file. This recording can also be accessed by navigating to “Programmable Voice” > “Recordings” in your Twilio Dashboard. Similar to Google Voice, you can delete the recorded file from this menu. This file is not secure or private. It is very similar to the way a traditional cellular provider or Google Voice would store voicemails available to your device.

If you would like Twilio to transcribe incoming voicemail messages and include the text spoken within your notification email, add “transcribe=”true”” within the “incomingvoice” TwiML Bin file. Mine appeared similar to the text below.

```
<?xml version="1.0" encoding="UTF-8"?>
<Response>
<Dial answerOnBridge="true" timeout="30" transcribe="true"
action="http://twimlets.com/voicemail?Email=your@emailhere.com">
<Sip>2125551212@2125551212.sip.us1.twilio.com</Sip>
</Dial>
</Response>
```

If desired, disable the “Request Inspector” logging feature within Twilio at “Programmable Voice” > “Settings” > “Request Inspector” > “Disabled” > “Save”. This does not stop Twilio from storing VOIP call metadata, but it does eliminate a small layer of internal logging.

As a reminder, all of the Twilio code presented during this section can be copied and pasted online from inteltechniques.com/EP. If everything is working well, you might consider adding more numbers to your strategy in order to have a selection for voice and text. We can add unlimited numbers which can be accessed through Linphone.

Keep in mind that additional numbers will extract funds faster. I only recommend additional numbers if you understand the reasons you need them. Repeat the previous steps for each number needed. While writing this update, I configured a toll-free number. The monthly fee for this number is \$2.00 (twice the price of a standard number), but it presents a more professional appearance.

You can now choose between multiple different numbers within your Linphone application. Whichever is chosen as default allows outgoing calls to be completed from that number. Incoming calls to any numbers will ring the app and allow connection regardless of the default account. Incoming text messages will be stored at the Twilio Dashboard and voicemail will be transcribed and sent to your email address. You could replicate this process for an unlimited supply of numbers, as long as you have the funding to support them.

While configuring Twilio within the Linphone application during testing of this strategy, I encountered several devices which presented authentication errors during usage. These usually claim that the Twilio credentials supplied to Linphone have failed and the user is prompted to enter the correct password. Supplying the appropriate password fails.

This appears to be an issue with Twilio temporarily blocking access due to too many invalid attempts, incorrect protocol settings, or launching and closing of Linphone from mobile devices too many times within a sixty minute threshold. Any account restrictions should reset after twenty minutes of inactivity. If your credentials stop working due to invalid login attempts, it is best to simply create new credentials as previously explained.

It is important to note that VOIP telephone calls and messages are not encrypted and we should expect no privacy. However, I have some isolation from my true identity. I use these numbers mostly for outgoing calls, such as calls to businesses. This strategy is an affordable option which allows telephone calls without relying on your cellular carrier-provided number. It can also be used to isolate outgoing “junk” calls which are likely to abuse your number. Twilio has the ability to see our logs, but so would any cellular carrier if we had made the calls via our official number.

The biggest feature of this process is the ability to possess affordable VOIP numbers on an Un-Googled operating system, such as GrapheneOS. We have granular control of our numbers without the need for Google’s services. I do not know of any other reliable VOIP strategy available for this private system.

I Hosting your own VOIP solution through Twilio eliminates the “middle-man”. There are many “burner” style services which give you free calls from a browser, but can pose great privacy risk. These include FireRTC, PopTox, and Globfone. Similar premium mobile apps such as Burner and Hushed can also pose similar dangers. Any time you allow a third-party service to facilitate your calls, you are also allowing them to intercept and see your data. All of these services rely on a VOIP provider such as Twilio, so I believe we should consider creating our own solutions and eliminate any additional companies which are unnecessary.

Apple devices rely on an Apple ID through the App Store and stock Google Android devices rely on a Google ID through the Play Store. Any apps you download for VOIP services leave a digital trail to your identifiers. Aliases can be used, but this method of VOIP with GrapheneOS gives us more control. This new VOIP strategy provides the missing services I desired for my own usage.

During testing, I attempted to replicate these services with Bandwidth LLC and Voip.ms. I do not recommend either of these companies. Bandwidth refused my numerous requests for service and Voip.ms demanded unredacted copies of my driver’s license before an account would be confirmed. When I refused, they closed my account which had a funded balance. While Twilio had their own roadblocks during account creation, they were the first VOIP service which actually provided me service. Anticipate fraud-related hurdles, but know that you can break through the temporary annoyances.

VOIP solutions often have limitations over traditional cellular communications. Twilio, and any services which rely on Twilio, do not support “short codes”. These are abbreviated phone numbers that are usually 5 or 6 digits in length. They are commonly used to send SMS and MMS messages with verification codes for account access. I avoid using this Linphone strategy for anything which will require text verification. I think of these numbers as landline replacements which allow me to send and receive voice calls. I always keep a single Google Voice account which can receive short codes. I explain more about this later.

My final warning about this strategy is that incoming calls can be an issue with some mobile devices. Outgoing voice calls should work flawlessly from any device, and this is my primary use for this service. I can easily place calls from my mobile devices or laptop (explained in the next chapter) at any time. However, incoming calls to mobile devices can vary, especially with Apple iOS devices.

If the iOS Linphone application is not active on the screen, it becomes dormant and stops monitoring incoming calls. You must activate the app in order to be notified of an incoming call. With iOS, be sure to disable “Push Notification” under “Settings” > (your number). If this toggle is enabled, calls will not come through even if the app is open.

With GrapheneOS, or any other Android device, Linphone stays open after initial launch and “listens” for incoming calls while inactive. This means you must launch the Linphone application once after each reboot in order to accept incoming calls. This behavior is also present on desktop environments, including Linux, which is desired. Fortunately, incoming Twilio calls consistently ring to the desktop Linphone application for all operating systems, including Linux, Windows, and Mac, as well as GrapheneOS devices. There are many variables with all of this, including the specific operating system builds and installed services. I often place hour-long calls from my laptop and incoming calls reliably prompt me to answer.

I have witnessed temporary number suspension from Twilio if Linphone on my GrapheneOS device is misconfigured. Since Linphone stays open and connected at all times, it may be synchronizing with Twilio servers too often with unique data. Disabling “Random port” under the “Settings” > “Network” menu and confirming “TLS” as the transport protocol in the “Settings” > (your number) menu should help avoid this error. If Twilio should ever terminate support for “TLS”, changing the protocol to “UDP” or “TCP” within Linphone may resolve the issue. If you continue to receive warnings about connections, you may need to contact Twilio support in order to identify the exact issue. Alternatively, opening the file menu and choosing “Quit” should eliminate multiple connections. However, this may impact incoming calls. Spend the time to correct the issue once for future usage without disruptions. In a moment, I present another service which is much less picky about these connection details.

By default, there is no name associated with the caller ID when you place a call from your Twilio number(s). This may be desired by some, but could be a disinformation campaign for others. On one of my Twilio numbers which I use for personal calls in my true identity, I attached my name to the caller ID. This way, my name appears as the caller on the screen of my bank or credit card company when I call from a Twilio number. It adds an extra layer of assurance. On another number, which I use with my alias name, I prefer that name to display as the caller. This also adds credibility to my call as an alias. Twilio requires you to contact their support in order to request these modifications.

As I write this chapter, Twilio is testing a new console design. Many of the features presented here are not available in it, which is frustrating. **If you are ever forced to use the new portal design, navigate to <https://twilio.com/console> or access the “Legacy” option.**

Overall, I view this method as a simple and affordable outgoing phone line which provides unlimited numbers at my disposal. I can place calls from my laptop or mobile devices when needed without ever exposing my true cellular number. I can accept incoming calls on my laptop or GrapheneOS device as if they were traditional landline telephones. While Twilio has served me well over the years, I now consider Telnyx to be a worthy replacement. Personally, I use both, but you should understand all options, as explained next. Later in the chapter, I summarize important considerations for all services.

Linphone/Telnyx VOIP Configuration

I have been using Twilio for many years because it was the only reliable VOIP option when I began this pursuit. Since then, I have discovered easier alternatives. If the Twilio tutorial did not generate the usage you desire, possibly due to a change in their menus or a suspended account, you might consider **Telnyx** (<https://refer.telnyx.com/zrfmo>). This VOIP provider replicates the service provided by Twilio, but their setup process is much easier. Now that you have an understanding of our Twilio strategy, I will abbreviate the steps here for Telnyx.

- Create a free account at <https://refer.telnyx.com/zrfmo> with \$20 in credits.
- Provide a custom domain email address, which is explained in the next chapter.
- If prompted for purpose, choose “SIP Trunking”.
- If prompted, leave the telephone number field empty.
- Click “SIP Connections” from the side menu.
- Click the “+ Add SIP Connection” button.
- Enter the name you wish to have for your connection (I chose “VOIP”).
- Enable “Credentials” as the “Connection Type”.
- Copy the username and password automatically generated.
- Click “Save and finish editing”.
- Click “Numbers” in the left menu.
- Enter a location, click “Search for numbers” then “Add to cart” for your number.
- Click the “Cart” in the upper right.
- Under “Connection or Application”, select your connection (mine was VOIP).
- Purchase the number using your free credits.
- Click “Outbound Voice Profiles” then “Add new profile”.
- Provide the name of “outgoingvoice” and click “Create”.
- Click “Outbound Voice Profiles” then the “Edit” icon next to “outgoingvoice”.
- Select your connection (VOIP) and click “Add Connection/Apps to Profile”.
- Click “SIP Connections” then “Outbound Options” to the right of the connection.
- Enter your new phone number in “Caller ID Override”, then click “Save”.

We are now ready to modify Linphone as we did previously. The following applies to any mobile or desktop platform using Telnyx as a VOIP service.

- Open the Linphone application and select the “Assistant” then “Use a SIP Account”.
- Enter the username previously provided by Telnyx; the new VOIP telephone number as the display name; “sip.telnyx.com” (US) as the SIP address; the password previously provided by Telnyx, and “TLS” as the protocol. Save everything and test.

Your Linphone application within your desktop or mobile environment (or both) can now make and receive calls without adding any funds. This is unique to Telnyx. **If you want to commit to Telnyx as your VOIP provider, be sure to add \$20 in new funds to your account in order to prevent termination of the trial.** This provides enough credits (\$40) to provide VOIP service for over three years, including a single number and usage.

Telnyx does not offer native SMS forwarding to their web portal or another number. The only option is self-hosting a forwarder to an email address as we did with Twilio. If you have your own domain and a shared web host, create a text file titled telnyx.php with the following content. Change “`your@email.com`” to the address where you want to receive notifications. Change “`@yourdomain.com`” to your actual domain name.

```
<?php  
$to = "your@email.com ";  
$subject = "Text Message from {$_REQUEST['From']} to {$_REQUEST['To']}";  
$message = "{$_REQUEST['Body']}";  
$headers = "From: telnyx@yourdomain.com ";  
mail($to, $subject, $message, $headers);
```

Upload the file to your host. The URL may be similar to `https://yourdomain.com/telnyx.php`. Within the Telnyx portal, conduct the following.

- Click “Messaging” then “Create your first profile”.
- Provide a name of “sms” and select “Twexit API”.
- In both “webhook” fields, enter the URL of the PHP file previously created.
- Click “Save” then click “Numbers” within the left menu.
- Within your number entry, select “sms” in the “Messaging profile” field.
- Confirm the rate notice if prompted.

Incoming text messages should now be forwarded to your email address. The subject will identify the sender and recipient while the message body will display the text message. This method prevents Telnyx from storing your incoming messages on their own server in the way that Twilio does. They would still have the ability to intercept and see the contents, but that is unlikely. Once the message is routed to your email, you should be the only host of the content. If you want to send a text from your new Telnyx number, click on “Messaging” in the Telnyx dashboard and click “Learn & Build” > “Send & Receive a Message”. You can use the online form to send a SMS text message to any number. You can also use the commands provided on that page to send messages from within Terminal. Similar to Twilio, I do not use this feature. I never use VOIP number for back-and-forth conversations. I only need to receive the occasional confirmation text message, which forwards to my email from both providers.

You can customize the caller ID name displayed during your outgoing calls within the Telnyx portal. Click “Numbers” from the menu and then “Caller ID/CNAM Listing” under the services area of your chosen number. Enable the “CNAM Listing” and “Caller ID Name” options, then enter any name desired. It may take a week to take effect. Be sure to enable two-factor authentication (2FA) through “My Account” in the “Security” section. 2FA options are presented in the next chapter.

While this configuration is simpler than Twilio, it also has less features. However, there are also benefits which are not available with Twilio. Consider the following.

- With Twilio, unanswered calls went directly to voicemail, and messages were transcribed and emailed to me. With Telnyx, unanswered calls disconnect after about one minute. There is a voicemail option, but it requires a third-party service or server. If you want voicemail and transcription, Twilio is the way to go.
- Twilio allows incoming text messages to be natively delivered directly to your dashboard or forwarded to any other number. Telnyx requires you to host your own message forwarding server for this to work. If you need the number to support incoming SMS text without third-party services, then Twilio is the appropriate option. If you have your own website, replicating this is fairly easy.
- Twilio possesses numerous fraud triggers which can impact our usage. Many readers report difficulties simply creating an account and being allowed access. Telnyx provides immediate access upon registration of a “business” email address.
- Twilio sometimes considers each opening of the Linphone app from iOS devices a new connection into their system. Ten open simultaneous connections within an hour results in a suspension of services until less than ten connections are present. If you only open the mobile or desktop app to make the occasional call throughout the day, this is no concern. If you minimize and open the iOS app every minute to make calls or check for service, you may experience problems. If your mobile iOS Twilio account keeps temporarily disconnecting, Telnyx might be a better fit. However, if properly configured, we should be able to avoid this. Using the transport protocol of “TLS” within Linphone should eliminate this problem.
- The pricing and overall call quality for Telnyx and Twilio is almost identical.

I currently maintain numbers through both services and configure each into all instances of Linphone. Both Twilio and Telnyx work great with mobile and desktop versions of Linphone. If I were forced to rely on only one service, it would be Twilio due to the voicemail options. If I needed access only to voice calls, I would choose Telnyx due to easy configuration and overall stability. Twilio often changes their settings without notice and support is practically non-existent. I experience more issues and outages with Twilio than Telnyx. Incoming SMS text messages from both services are forwarded to my email account via my website. In a moment, I provide further summary of detailed usage of all services for myself and clients.

MySudo VOIP Configuration

Many of my clients currently use the VOIP service **MySudo** (mysudo.com) for most non-secure communications, such as incoming and outgoing telephone calls. 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 device, and each can be used for incoming and outgoing calls and text messages. It requires a traditional iPhone or Android device. It does not currently work on our GrapheneOS device because MySudo requires Google Services. MySudo does not need your name, email address, or telephone number. The installation is unique to your hardware. MySudo only knows you by this “fingerprint”, which has no association to your true identity. You should be able to obtain a free trial, and purchase any premium plans anonymously using the methods discussed later. This app currently only works on a mobile device. However, it can replicate to a secondary device, such as an iPod Touch. Note that a single number plan provides incoming and outgoing calls and texts for less than the price of a number from Twilio or Telnyx. The following is my strategy for the nine VOIP numbers.

- 1: Personal (Real Name): This is for friends and family who do not use secure communications (telephone only). When they adopt MySudo, I can still use this line for encrypted communications.
- 2: Google Voice Forwarding (Real Name): All of my old Google Voice numbers forward all calls and text messages to this single number (explained later). I can now answer all 35 of my old numbers in case a call should come through. This is beneficial when friends and colleagues from many years ago try to contact me through an old Google Voice number which I have given them. Google knows these were all me.
- 3: Home (Alias Name): This name, number, and email address are unique to anything that involves my home. Utilities, services, maintenance, neighbors, and all house-purchase paperwork connects to this profile. When that line rings, I know to answer as my home alias.
- 4: Business (Real Name): When I need to deal with any business-related phone call, I use this profile. This number has been leaked to business lookup websites. The email address is used for any business-related registration I must complete which will ultimately send me spam.
- 5: PMB (Real Name): You will learn how a PMB in another state can help create a great layer of privacy. This number is local to the area of my primary PMB and allows me to really “sell” it.
- 6: Social (Alias Name): As mentioned previously, being anonymous does not mean you can’t live a normal life. This number is used for any social activities near my home. New friends I meet under my new alias have this number for me.
- 7-9: Due to my own privacy concerns, I do not disclose the specifics of these accounts.

Number Porting

Now that you have a new mobile device with new anonymous service, you likely need to 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 Google Voice 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 Twilio, Telnyx, MySudo, or Google Voice 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.

As you may recall, I am not a fan of Google products from a privacy perspective. However, Google Voice is our current best option for porting numbers. Once we have the process in place, there will be no need to log in to the Google account, and you will never do so from your new clean device. Google will receive information about your communications through their service, but I do not see it as any worse than your previous telephone carrier possessing the same data.

The first consideration is to identify which Google account to use for the porting. If you have never had a Google account, you have no choice but to create a new one. Many people may think that a new account should be mandatory for this procedure, but I have a different view. Google can be cautious when it comes to new accounts. If you create an account from a VPN using a burner email address, Google might find this suspicious and suspend the account until you upload government identification proving your identity. I find this invasive. I respect their need to block usage from spammers, scammers, and other crooks, but I do not want to have my own account suspended. If you already have a Google account established in your true name, and your old phone was also established in your true name, I see no reason why you should not pair these together.

Remember, our goal is to configure a system to receive calls and messages from a number that was already associated with your true identity. Connecting this to a Google account under your true identity does not gain or lose much privacy at this point. I would rather attach your old number to an aged Google account that has very little risk of being suspended due to questionable activity than to connect it to a brand-new account which will be scrutinized by Google.

If you have an old Google account in your name, I suggest using that. If you have no account, I would create an account in your true name. This may sound ridiculous from a privacy perspective, but if it gets suspended, you have a much better chance unlocking it when you are the person with whom it is registered. It will receive extremely minimal use, and Google will collect very little information from it. Let's get started.

- Find your billing account information from your current service provider, such as your account number and PIN. You need this information to complete your port request.
- Within a web browser while protected by your VPN, navigate to voice.google.com.
- Sign in with your Google account credentials if you are not automatically logged in.
- If you haven't used Google Voice on your account before, set up a new Google Voice account. You'll be prompted to pick a new number, but your ported number will soon

replace it, so it won't matter what that number is. You can use your old cell number as your verification number, as it is still active on the old device.

- At the top right, click "Settings".
- Click "Transfer" under your number.
- Next to your current number, click "Change / Port".
- Select "I want to use my mobile number". Follow the onscreen instructions to set up your new number and pay. Google will charge a \$10 fee for the porting. You might be charged a \$20 fee to port your mobile number to Google Voice from some mobile service providers, such as Verizon or AT&T. Since your account is already in your true name, I provide a traditional credit card during purchase.
- Continuously check the status of your number porting. Numbers typically take from 48 to 96 hours to port.
- Don't cancel your phone plan until Google notifies you the port is complete. To verify the port, they will call your phone with a code. After the port is finished, your service provider will cancel your phone service.
- If you have multiple numbers on the original account, check with the service provider first to find out about their policies. If you want to keep the plan and get a new mobile number, confirm that with the service provider.

Once you see your old number which was previously attached to your cellular telephone appear as your new number in the Google Voice account, the porting is complete. Test this by completing the following steps.

- While logged in to your Google account, navigate to mail.google.com.
- Navigate to www.callmylostphone.com and enter your telephone number.
- On the Gmail screen, you should see an incoming call.

There is no need to answer this call, you just want to make sure that the number can receive calls through Google Voice. You are finished with this step. If anyone from your past calls your old number, you have a way to receive notification of the call. This applies to text messages as well. You have control of the number. If you need to make a call from that number, such as to prove your identity to a bank, you can make calls from the Gmail or Voice pages while logged in to the Google account in a web browser. Having the ability to occasionally check the Google account may be all you need. Personally, I do not like logging in to Google products, so I take advantage of their forwarding options, as explained next.

It should be noted that Twilio, Telnyx, and MySudo also offer number porting options into their network. At the time of this writing, I have not tested this feature. I believe Google Voice is still the best option which will not generate monthly fees for access to the number. It also allows us strong security with two-factor authentication.

Number Forwarding

I mentioned previously that one of my VOIP numbers is for Google Voice forwarding. Over the years, I have accumulated many numbers from Google Voice. Some of these are heavily associated with my true name. As an example, I used a Google Voice number when I worked as a Detective at a police department. We were all required to disclose our cell numbers on a callout list, and I only provided a Google Voice account. To this day, I hear from former colleagues through that number. Many of them assume it is my cell number, and I have no need to correct them. While I have moved all of the people with whom I continuously communicate over to better options, this Google number still receives a lot of activity. The following explains how I interact with these numbers without using the official Google websites or apps.

First, let's assume that you have either a Twilio, Telnyx, or MySudo VOIP number of 202-555-1111 and email address of voip@protonmail.com. Any calls to that number will ring your phone through your VOIP provider and incoming emails will be received within your ProtonMail inbox. Your telephone carrier and manufacturer will not know of these calls or messages. Next, conduct the following.

- In your web browser, navigate to voice.google.com and select “Settings”. Your Google Voice number could be the old cell number which you ported into Google.
- The “Linked Numbers” section should either be blank or possess the same number as your previous cell number. Remove any numbers within this block.
- Add a “New linked number” of your VOIP number for forwarding (202-555-1111).
- Confirm the code sent via SMS text to that number.
- In the “Messages” section, ensure that messages are forwarded to the Gmail account connected to this profile.
- In the “Calls” section, ensure that call forwarding is enabled.
- In the “Calls” section, ensure that “Get email alerts for missed calls” is enabled.
- In the “Voicemail” section, ensure that “Get voicemail via email” is enabled.

Let's pause and think about what is in place now. If anyone calls your old cell number, which was ported to Google Voice, the call is routed through Google Voice and then to your VOIP number. Your VOIP number will ring as normal and you can accept the call. The caller ID will show the number calling you. If you decline the call, the caller will be sent to your VOIP voicemail (if available). If you simply do not answer, it will be sent to the Google Voice voicemail. If he or she leaves a voice message within your Google Voice account, it will forward to your Gmail (which we will soon forward to ProtonMail). If someone sends you a SMS text message to this old number, it will also be received in the email account. Now, let's forward those messages in order to prevent checking the Gmail account at all.

- Navigate to gmail.com while logged in to the account associated with the old number.
- Click the gear icon on the right and select “Settings”.
- Click the “Forwarding and POP/IMAP” option in the upper menu.
- Click “Add a Forwarding Address” and enter the desired email address.
- Google will send a confirmation email to your account.
- You should now have the option to select “Forward a copy of incoming mail to” and choose your email address in the drop-down menu. Choose “Delete Gmail’s copy” and save your changes.

Now, when someone leaves you a voicemail or sends you a text message to the Google Voice number, it will appear in your primary email and Google will delete the original after 30 days. You can now receive calls, voicemails, and text messages from your old number within your VOIP and email strategies without ever logging in to Google again. You can also respond to text messages via your email address and the recipient will only see the previous cellular number that is now assigned to Google Voice. I don’t recommend this since the message is sent on behalf of Google.

It is vital to test all of these options before relying on them. If you have VOIP, test all calling and texting options and make sure everything appears as desired. If you do not have a VOIP solution, let’s repeat the entire process with alternative options.

- In your web browser, navigate to voice.google.com, click on the left menu, and select “Settings”. Your Google Voice number should be the old cell number which you ported into Google.
- The “Linked Devices” section should either be blank or possess the same number as your previous cell number. Remove any numbers within this block by clicking the “X” next to each.
- In the “Messages” section, ensure that messages are forwarded to the Gmail account connected to this profile.
- In the “Calls” section, ensure that “Get email alerts for missed calls” is enabled.
- In the “Voicemail” section, ensure that “Get voicemail via email” is enabled.

If anyone calls your old number, the call is routed through Google Voice and then immediately to voicemail (unless you are logged in to Google Voice via web browser). If he or she leaves a message, your email account will receive the audio and text version of the call. If someone sends you a SMS text message to this old number, it will be received in the email account as well. Now, let’s forward those messages in order to prevent checking the Gmail account at all.

- Navigate to gmail.com while logged in to the account associated with the old number.
- Click the gear icon on the right and select “Settings”.

- Click the “Forwarding and POP/IMAP” option in the upper menu.
- Click “Add a Forwarding Address” and enter your email address.
- Google will send a confirmation email to your account.
- You should now have the option to select “Forward a copy of incoming mail to” and choose your email address in the drop-down menu. Choose “Delete Gmail’s copy” and save your changes.

Now, when someone leaves you a voicemail or sends you a text message, it will appear in your email account and Google will delete the original after 30 days. You cannot receive calls, but will be notified of voicemails and text messages from your old number without ever logging in to Google again. You can also respond to text messages via your email address and the recipient will only see the previous cellular number that is now assigned to Google Voice. Again, this should be tested before actual use.

I have replicated this process across many of my old Google Voice numbers. This may seem sloppy, as Google now knows I am the owner of all of the accounts. My stance on this is that it likely does not matter. Google probably already knows. Their heavy use of browser fingerprinting, analytics, and IP documentation allows them to know when people use multiple accounts. Since I no longer have these numbers as part of my normal usage, I consider them all “burned” and only wish to have the ability to receive any notifications. Note that Google allows any VOIP number to be connected with only one Google account. We can no longer forward multiple numbers to a single VOIP number. We can also no longer forward SMS text messages to other VOIP numbers, but I never used this feature anyway.

If you call any of my old numbers, my primary device receives the call through various VOIP numbers. If you send a text to any of my old numbers, they are received in my email inbox. I never use these Google accounts to make any outgoing calls or send texts. These are only used for incoming content from people who do not know my true new number(s).

This presents a small annoyance with this plan. You can only call out from your old Google Voice numbers if you log in to the corresponding Google account. I try to avoid this unless the caller ID on the other end needs to be the old Google Voice number. There are a few reasons you may need to do this. Imagine that you contact your credit card company in reference to your account. The cellular telephone number that they have on file is your previous Google Voice account. For security purposes, they mandate that you contact them from a known number to protect your account. You could call from the Google Voice dashboard and the number would be sent through via caller ID. If you do need this outgoing call feature, consider associating a dedicate browser for this purpose. Brave is based on Chromium (Chrome) and works well with Google Voice. I prefer to eliminate association with any Google accounts within my primary browser, which is Firefox as explained later.

Telephone Number Considerations

Are you confused yet? With so many options, I find the complexity of choice within telephone communications to be a real issue. Twilio, Telnyx, MySudo, Google Voice, and traditional numbers present numerous usage options. Overall, I hope these previous guides help you determine your own usage strategy. However, I want to present one final summary of how I use these services for myself and clients. I think this may help your own decisions.

I carry a GrapheneOS Android mobile device while traveling. It has a SIM card with a true cellular number, but I never use it for calls or texts. I have Linphone installed on the device and two VOIP numbers configured. One is through Twilio and the other through Telnyx. I can make calls from either of them, and both numbers ring directly to the device. Both numbers are also connected to my home laptop. I leave Linphone open on my laptop all day, and it reliably notifies me of incoming calls. I have an old Google Voice number which is required by some banks due to the history of use. I never make calls from it, but I have forwarded all incoming calls to a VOIP number. If my credit card company insists on calling me at a known number, I can receive a call through Linphone via VOIP, originally from Google Voice. Google has a log of the call, but no details about duration. All incoming text messages are forwarded to my email. I have MySudo on my secondary iPod Touch device which is used as previously outlined. I have 12 numbers total.

I deviate a bit from my own strategy with clients. Many also receive a GrapheneOS device with Linphone, but most only need one Twilio or Telnyx number. They use it for all traditional incoming and outgoing calls and never use their newly-assigned cellular number. Their laptop is also configured for incoming and outgoing calls with this number. The number can be abused any way desired, and is the line used for all traditional phone calls. All text messages are forwarded to their email via my web server. I then create a new Google Voice account. When prompted to enter a valid cellular number, I provide their previous true number associated with their old phone (which still has service). I then add the Twilio number to this Google account as a secondary number. When I am ready to shut off their old service, I port that previous cellular number to the Google Voice account. I configure this Google Voice account to forward any incoming text messages to an email account. This way, an incoming text to their old cell number is routed to email. This message can be read regardless of location. The Google Voice number is provided any time a telephone number is required for Two-Factor Authentication (2FA, which is explained later). The Google account is secured with a YubiKey (also explained later). The likelihood of an attack toward Google is much less than the abilities with a standard cellular number. The text codes arrive securely within an email account, which can be accessed from anywhere. Google Voice also supports text messages from short code numbers.

If you are using Linphone for VOIP with either Twilio or Telnyx, you may run into unique complications. Regardless of the chosen service provider, while using either the mobile or desktop application, I make sure the following options are configured within the settings menu for each number. I have witnessed these settings default to one option on a desktop while randomly changing on another version, such as a mobile device. If you experience broken connections, check the following first.

- Register: Enabled
- Publish Presence Information: Enabled
- AVPF: Disabled
- ICE: Disabled
- Turn: Disabled
- Encryption: None
- Outbound Proxy: Disabled
- Push Notifications: Disabled
- Settings > Network > Use Random Ports: Disable

For clients who insist on an Apple mobile device which is by their side at all times, I simply install and configure MySudo for their telephone needs. It is the easiest option and simply “works” at all times. Text messages and calls are reliable without any additional effort. If they plan to use a Faraday bag to isolate their phone from their home, as explained later, I configure a secondary iPod Touch which contains the same MySudo application, configuration, and telephone numbers. This varies by client, but most prefer MySudo over Linphone. If you do not enjoy tinkering and troubleshooting, and just want a functioning device without any worries, then MySudo is your best option. If you want desktop calls, you need Linphone. If MySudo begins supporting GrapheneOS and desktop calling, I will revisit my entire plan.

I offer one final consideration for any mobile VOIP/Linphone strategy. The Linphone software accepts multiple numbers for incoming and outgoing calls. However, their menu is quirky and only allows you to place outgoing calls from the most recently added (default) number. You can select the default number for outgoing calls within the “Settings” menu. In there, select the desired outgoing call account and enable “Use as default”. The laptop application, which is explained in the next chapter, does not have this issue. You can select any number and make a call from that account easily. If you only associate a single VOIP number to your device, none of this matters. Again, most of my clients only need one number to facilitate outgoing calls without exposing their true cellular number.

Overall, try every service by taking advantage of free trials and identify the option best for you. Things change quickly with technology and you may find my results inaccurate.

VOIP Acceptance Issues

VOIP numbers work great for incoming and outgoing calls. They can work well forwarding incoming text messages to email if you are willing to configure the options. Outgoing text messages can be a pain unless you are using MySudo or Google Voice. 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, but I have some solutions.

If you ported your true cellular number to a VOIP provider, such as Google Voice, Twilio, Telnyx, or MySudo, that number will probably pass VOIP scrutiny for several months. This is because banks and other online services query the provider number through a carrier identification service. These are notoriously outdated and your ported number will appear to be associated with a true cellular provider for some time. Even though you may have ported a number from AT&T into Google Voice, the carrier ID will display AT&T until various databases are updated. I currently have a ported number which passes scrutiny on every online service I have tried (for now).

We can apply this strategy with new numbers in many scenarios. The following are the steps I recently took in order to provide a client a VOIP number which would appear to be associated with a true cellular number. These steps are often blocked due to abuse, but hopefully you will be able to replicate something similar.

- Activate a Mint Mobile SIM card for a one-week trial.
- Immediately purchase one month of access.
- Two weeks after the purchased plan begins, port the number to your desired VOIP provider, such as Google Voice, Twilio, Telnyx, or MySudo.

These actions will cancel the Mint Mobile account. When you provide the number issued by Mint to any online service, it will appear to be associated with T-Mobile. This association should last between one and six months (sometimes longer). Immediately attach this number to any desired online accounts. Once the number is confirmed, they should never check carrier records again.

Mint does not like this behavior and may block you from porting a number. If they do, wait until the next billing cycle and try again. Ultimately, they must allow you to take your business (and your number) somewhere else.

Secure Messaging Configuration

You should now have a new device that has no connection to you. It possesses prepaid cellular service with no name attached. Since you do not use the number provided by Mint Mobile for any communications, they have 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. All of your outgoing calls are made through VOIP numbers, which may not know your true identity. 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.

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 a huge amount of 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. My requirements for a secure communications service include all the following.

Zero knowledge, End-To-End Encrypted (E2EE): 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.

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 very unlikely. Compare this to a traditional telephone provider which 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.

Secure Communication with Signal

There are things I do not like about Signal (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 is a huge privacy violation. You must then give out this number in order to communicate with others securely. This shares your number in a way we typically try to avoid. If you choose to use Signal, you should create an account associated with a VOIP number, as previously explained, such as a Twilio, Telnyx, MySudo, or Google Voice number. I typically prefer to use a client's previous personal number which has been ported to Google Voice for this use since it may already be known by others in their circle. This shares the VOIP number with all contacts, but that does not expose the new true cellular number. Using this old number can make communications easier and more trusted by the other party. Never use your true cellular number with Signal.

Signal notifies people when one of their contacts creates an account. This may be beneficial to you if your ported Google Voice number is already trusted by your friends. If you do not like this feature (I do not), you might consider using a brand new VOIP number unknown to anyone else. This eliminates any contacts knowing you are now on Signal. I created a VOIP number which is only used to establish communications with others through Signal. This may be unnecessary for you. Let's walk through a typical configuration of Signal.

- Download the Signal app through Aurora Store (GrapheneOS) or App Store (iOS).
- Launch the app and accept the default requirements.
- Enter a VOIP number and confirm a text message or voice call.
- Provide a desired first name, which can be a single letter.
- Enter a secure PIN.
- GrapheneOS users: 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.

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 we will install in the next chapter.

If you are using GrapheneOS, 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 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 the “Account” option and enable “Registration Lock”. This requires your Signal PIN to register a new device.
- Tap the back button and open the “Privacy” menu.
- Enable “Screen lock” if desired. This forces a fingerprint or PIN to open Signal.
- Disable “Show Calls in Recents” to prevent call details from being stored within the operating system.
- Disable PIN reminders if desired.
- Click “Advanced” and disable “Allow from Anyone” if desired. This prevents any unsolicited contact but may prevent desired communications.
- Disable “Show Status Icon” to hide your availability.
- Tap the back arrow twice to return to the “Settings” menu.
- Tap “Chats” and disable “Generate Link Previews” to prevent loading of websites.
- Tap the back arrow to return to the “Settings” menu.
- Tap “SMS and MMS” (Android) and enable Signal as default messaging application.

When you participate in a conversation with someone on Signal, tap their name on the top menu to access settings for them. Consider enabling “Disappearing Messages” and choosing an appropriate length of time. I typically enable “1 week” for all contacts. A week after I send any message, it is permanently erased from both devices.

Signal is far from perfect. Many elitists insist on using robust 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.

Secure Communication with Wire

Wire (app.wire.com) is my second preferred secure messenger over all others. While 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, and I recommend a ProtonMail address for this purpose, as explained later.

Wire has native applications for iOS, Android, Windows, macOS, and Linux. GrapheneOS users can download through Aurora Store. If you are using any other system, you can also connect via their website within a browser. Regardless of your connection, 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.

I do have minor 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. Next, Wire seems to purposely make it difficult to find the free version. Visiting wire.com only presents their paid tiers. Visiting app.wire.com and selecting “Personal” allows a free account creation. This is also not a huge deal, but it should be acknowledged when introducing the service to others.

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. One unique feature of Wire is the ability to configure up to three user accounts within the application. On both my mobile and desktop versions of Wire, I have the same three accounts which I can use for various purposes. This alone justifies Wire as one of my preferred services. Note that Wire does not receive notifications within GrapheneOS.

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, MySudo, or most other secure messaging options. I am not concerned with the location of their HQ. 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.

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. Consider the following.

- **MySudo** (mysudo.com) offers free secure communications within their network. This includes E2EE text, audio, and video. If the majority of your contacts already have MySudo for their VOIP solution as previously explained, then this may be the only secure option you need. It did not make the “top two” because of lower adoption and no ability to place calls through a browser or desktop application (or GrapheneOS). This is vital for clients who do not bring a mobile device into their homes.
- **Session** (getsession.org) has possibly the most private text messaging options, but adoption is extremely low and voice calling is not supported.
- **Matrix** (matrix.org) is a phenomenal open-source and decentralized platform, but their focus is on community chat rooms for a niche tech-savvy audience.
- **Threema** (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) 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.
- **NOT RECOMMENDED - Wickr** was the first secure communications application I ever used. It still works well and I believe their encryption is safe. However, I stopped using the service in 2020 when I discovered that they were sharing user details with third party services including Microsoft and Google. I spoke with the CTO of the company who confirmed that analytical data and IP addresses of all users are shared with these companies. I find this unacceptable and encourage others to move to more privacy-respecting options.
- **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 E2EE 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.

VPN Configuration (Mobile)

Virtual Private Networks (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. I break this down further in the next chapter.

Virtual Private Networks 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 currently recommend ProtonVPN. Navigate to inteltechniques.com/proton for further information and the best purchase links. The current rate for ProtonVPN ranges from free (slow) to \$96 per year (fast). Most clients use the "Basic" tier of ProtonVPN at \$48 annually. It includes unlimited use, connection to two devices simultaneously, and fast speeds. If you have gigabit internet speed in your home with many devices, the top tier may be more appropriate. Consider the packages which include both ProtonVPN and ProtonMail for the best deal. Configuration of a VPN on your mobile device can be extremely easy or somewhat challenging, depending on your level of paranoia. Let's approach this from two levels.

Basic: For most readers, and almost every client I have consulted, I recommend sticking with the standard application provided by the VPN company. These branded apps should suffice for most needs. ProtonVPN can be downloaded from the App Store, Google Play, or F-Droid on GrapheneOS. Once installed, simply provide your account credentials and launch your VPN connection. This was my personal choice for many years.

Advanced: Some VPN apps are closed source. This means that we cannot truly know what the app is doing behind our backs. While most reputable VPN companies have our best interests in mind, we must always be cautious. This is one of many reasons I encourage people to research the OpenVPN application. This free open-source mobile app allows you to configure multiple VPN clients within one location. If you have subscriptions to more than one service, you can configure each within the app and select the desired provider and server

upon each connection. Configuration will require some research, but most VPN companies provide explicit instructions for this option. If you only use ProtonVPN, I recommend their traditional app. There is no need for third-party software.

Another option is to manually configure your VPN through your mobile device's system settings. With iOS, I can specify the exact VPN details and make a connection without any third-party software. At the time of this writing, full instructions for ProtonVPN were available on their website at <https://protonvpn.com/support/protonvpn-ios-manual-ikev2-vpn-setup>. This option uses the IKEv2/IPSec protocol, which is built into iOS. Most will agree that OpenVPN provides slightly more secure encryption, but it requires a third-party app. IKEv2/IPSec does not require an app, but has slightly weaker encryption. Again, if using ProtonVPN, stick with their app. I simply want you to know of all options.

What should you choose? If the terms OpenVPN, IPSec, and IKEv2 mean nothing to you, then you should stick with the basic option and use your VPN provider's mobile application. It offers a very secure environment, but you may give up a bit of privacy in rare scenarios. Fortunately, ProtonVPN has made all of their applications completely open-source. This makes it much more difficult to hide malicious programming within the code. If you do not want to install third-party apps and want to use a VPN directly through your mobile operating system, the advanced option may be desired. I encourage you to test them all and learn the protocols. Overall, ANY of these options, while using a reputable provider, beats no VPN at all.

My VPN policy is quite simple, but my opinions about VPN companies can be complex. Any time that I am connected to the internet from my laptop, desktop, or mobile device, I am connected through my VPN. I know that my internet traffic is encrypted and originating from an IP address not associated with me. I never deviate from this policy. I believe that every reader should consider a paid VPN. In a later chapter, I will present a more hardened home solution for a constant VPN in your home. In the next chapter, I share more insight on the use of VPNs for privacy within desktop environments.

What do I use? I rely 100% on ProtonVPN through their app on my mobile device and laptop(s) while I am traveling. Home devices are protected through a firewall with ProtonVPN, as explained in Chapter Four. I trust them more than most commercial options and I believe their business model is the most transparent. Being hosted in Switzerland provides some aspect of privacy from vague government intrusion, but international servers could always be compromised.

Any updates in regard to my VPN recommendations will be posted on my website at inteltechniques.com/vpn.html. Throughout the remaining chapters, I will present more information about VPN usage and services.

Device Backup and Restoration

In the previous edition of this book, I explained the process of installing LineageOS as a custom Android operating system and the ability to archive backups for easy restoration. I no longer present LineageOS as an option and GrapheneOS does not have any native backup solutions. However, I don't necessarily recommend this today anyway.

During years of explaining the backup and restore options within Android, I have never had a successful restoration. If you have an issue with your GrapheneOS device, it is simple to repeat the previous installation tutorial while gaining the benefit of an updated system. Since we only want minimal required apps on our devices, installing and configuring them should not take long. The short summary with Android is to avoid full backups, and simply rebuild whenever necessary. However, make sure you have copies of any photos, documents, or other important data before wiping the device.

My feelings are different with Apple products. Backing up your iPhone is much easier than Android. It only requires you to open Finder on your new Apple computer with Catalina, Big Sur, or later operating system, connect the mobile device via USB, and conduct the following.

- Click the phone option in the left menu.
- Scroll down and click the “Back Up Now” button.

This will create a backup of the operating system configuration and all Apple data such as your contacts, notes, and calendars. 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 I will not be with them when a disaster happens.

In 2021, I purchased a new replacement iPod Touch as my secondary home device. Usually, I would make a fresh start with a new Apple ID, but I wanted to test my backup strategy. I turned the new device on; chose the computer connection option; connected it to my MacBook Pro; launched Finder; selected the device; and chose the option to “Restore Backup”. Within a few minutes, I possessed a new iOS device which contained the same configuration as the previous device. I then launched iMazing and transferred the data from the previous device to the new replacement to create a true clone. To be fair, I could have downloaded all of my desired apps within the same amount of time. Today I insist that all of my clients possess a valid backup of their apple devices, ready for easy restoration.

Secondary Device Configuration

Your new private Android or iPhone may be all you need in regard to a mobile device. Most people carry it with them everywhere they go and leave it connected to the mobile network at all times. I believe this is risky behavior and a desire for extreme privacy will require you to take more extreme action. My primary mobile device has never entered my home and has never connected to a cellular tower within five miles of my house. While unlikely to happen, it prevents my phone from announcing my home location. If someone did figure out my mobile number, and paid a bounty hunter or private investigator to locate my device, it would not lead anyone back to my home. The last known location would be a busy intersection with no connection to me. You can accomplish this and still possess a mobile device in your home with all of the communication apps you need with the following instructions.

When I am traveling, my phone is always by my side and is my primary means of secure communications. When I return home, things change. When I am about five miles away from my home, at a very specific location, I drop my device into a Faraday bag. This shielded pouch (amzn.to/3gmNjZ) prevents any signals from reaching or leaving my phone. It stops communications with cellular towers. The device stays in this bag until I am at least five miles from my home heading out on another trip. Since the phone is never connected to any network while near my home, it cannot reveal the location of the device (or my home).

While at home, I can still possess a mobile device for my secure communications. I use an iPod Touch for this. The iPod Touch possesses the same iOS operating system as the iPhone. It connects to my wireless network in the home (behind a firewall with VPN as discussed later) and has internet access, but no cellular connectivity. It possesses a unique Apple ID never used on any other device. Most secure communication apps, such as Wire, work the same as on my primary phone and can share accounts. Neither Apple or Google will know this association. Linphone can be configured with the same VOIP number(s) using the previous tutorial. This way, I can send and receive calls and texts associated with this number at all times. Configuring Linphone on my laptop with the same account details offers yet another avenue for standard voice and text communication. All three devices have the same number(s). I should note that 50% of my clients do not use a secondary mobile device in their homes and rely on their laptop for communications. The other half use this strategy in order to possess a small device within the home without the need to rely on a large laptop all day.

If you use an iPhone as your mobile device, MySudo can possess the same telephone numbers for incoming and outgoing calls across all devices. In order to replicate an installation of MySudo, and share the same numbers across two devices, both devices must be active at the same time during configuration. I must scan a barcode from my primary device with my iPod Touch. Both devices need internet access during this process. Therefore, I set all of this up on public Wi-Fi behind a VPN before taking the iPod Touch to a client's home. This is a one-

time exception. First, I enable power on the iPod Touch at any library with free Wi-Fi and allow my cellular telephone to be connected to a cellular data connection. I configure everything on the secondary device as needed, which will require access to the primary device to allow these connections. I then “forget” the Wi-Fi network on the iPod Touch. An optional step here is to tell the device to forget all networks, if desired. I then turn it off completely.

If you use the GrapheneOS option, this does not apply. You could set up MySudo on your “Home” device and rely on Linphone while mobile. That is what I do, but I also configure Linphone on my iPod Touch and laptop. This gives the best of both worlds while at home. Upon arriving home, I connect the iPod Touch to my home Wi-Fi (behind a VPN firewall as explained later) and it never leaves the house again. This secondary device replicates all communications options I need. Aside from lack of a cellular-provided number and service, it appears identical to my “phone”. Since Pixel devices are required for GrapheneOS, and they all have embedded cellular chips, I do not recommend a secondary GrapheneOS home unit.

Another issue with this plan is the installation of Signal on the secondary device. Unlike username-based services such as Wire, Signal relies on a telephone number. Furthermore, it only allows usage on one mobile device at any given time. However, it provides a desktop application which can be used on multiple machines. Therefore, my secondary mobile device (iPod Touch) does not possess my primary Signal account, but my primary laptop does. I can send and receive text, audio, and video over Signal while using this laptop.

I insist on preventing any devices from connecting to any cellular network while in my home. These connections can immediately identify someone’s location. The iPod Touch has no cellular connectivity. It never leaves the home and never connects to any other network. I think of it as my landline which only functions in the home. If you possess an anonymous telephone with prepaid service and an anonymous Wi-Fi only device, both of which have no connection to your identity or each other, you have an amazing layer of privacy protection.

If you go through the troubles of obtaining an anonymous home as discussed later, these steps are vital so that you do not expose yourself. Airplane mode is not enough. System updates often disable airplane mode on reboot. It only takes one accidental connection to create a permanent record of the location of a device. These steps prevent unintentional exposure that could ruin all of your hard work. Some readers of the previous edition expressed concerns of Apple eliminating the iPod Touch from its lineup of mobile devices. Fortunately, they released a 7th edition in 2019. This device supports the current version of iOS (14). Based on previous support models, I expect the latest iPod Touch to receive support updates through 2023. You should note that all iPod Touch models lack Touch ID, Face ID, 3D Touch, NFC, GPS, an earpiece speaker and a noise-canceling microphone. However, all communication functions work well with a set of earbuds which contain an in-line microphone (such as those included with most older iPhones).

Faraday Bag Selection and Testing

I insist on thoroughly testing any Faraday bags I purchase. Over the past ten years, I have acquired at least five 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 voice mail. 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.
- Play music from the device to the speaker.
- While music is playing, drop the mobile device into the bag and seal it.
- After the previous test, with music playing, drop the speaker into the bag and seal it while the mobile device is NOT in the bag.

In both scenarios, 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. I also believe you should test the other connections as explained above. A Faraday bag should never be used before thorough 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. I currently rely on the Silent Pocket nylon bag (amzn.to/3gmNjNz) for my GrapheneOS device. Silent Pocket offers a discount to listeners of my podcast at <https://silent-pocket.com/discount/IntelTechniques>, and my show receives small affiliate payments from purchases. I sought this relationship after using the products.

Mobile Device Usage

Now that you have an anonymous telephone and possibly an isolated Wi-Fi only “Home” phone, we should have a conversation about general usage. I believe that we should all use mobile devices as they were originally intended, as a means of necessary communication. I do not believe privacy-conscious people should ever consider a mobile phone as an entertainment device. It should not be used for games, video streaming, or extensive web browsing. We should be very reserved with the applications installed on these clean devices. Most clients’ two iOS devices are almost identical as far as application presence. While they have unique Apple IDs, the usage and setup are quite similar. Those who possess an Android for mobile use an iPod Touch for home see many similarities between the two, but recognize minor differences in the convenience of each. Consider the following.

Telephone: As explained previously, I rely heavily on the Linphone app on both devices. It allows me to replicate my account on my second Wi-Fi device so that I can make and receive calls from any of my VOIP numbers. At home on my iPod Touch, I also have nine numbers through MySudo at my disposal with the highest plan.

Email: I use the standard ProtonMail application and connect my premium account to each device. This allows me to send and receive secure emails from multiple ProtonMail addresses as well as accounts associated with domain names which I own. We tackle ProtonMail soon.

Secure Messengers: I rely on Signal and Wire for secure communications with clients. The Wire software on both mobile devices and my laptop is connected to all three Wire accounts. This allows seamless communication. My mobile device and home laptop share a Signal account for consistent communications on that platform. I maintain an emergency Signal account on my iPod Touch device if ever needed, but it is rarely used.

VPN: I have the ProtonVPN app on both mobile devices, but I leave it disabled on the home unit because it is protected by my home firewall (explained later). While traveling, I leave the ProtonVPN application executed and connected at all times with the “Always-On” option enabled. This is not a true kill-switch as you may see within desktop applications, but it is the best option we have with Android and iOS products.

These apps allow me to communicate securely via email, encrypted text, encrypted voice, encrypted video, and traditional VOIP telephone service. I have every avenue of communication covered, and each device allows full use through all of my accounts. The end user does not know which device I am using. My cellular service provider knows absolutely nothing about my activity, only the amount of data used. T-Mobile also has no record of any calls or text messages, and does not know the name attached to the account. Neither Apple nor Google know the details of each account or the VOIP numbers being used.

Web Browser: Your choice and configuration of a web browser on your desktop computer is very important, and is explained in detail in the next chapter. If using GrapheneOS, I recommend the included hardened browser Vanadium. Your privacy and security options within the Apple iOS and stock Android operating systems are more limited. Apple mandates that any third-party browsers rely on its own rendering engine. This means that every browser on an iPhone is still using Apple's code, regardless of the brand. Chrome, Firefox, and every privacy-themed option is still using Apple's internal browser software. Android allows more options, but pushes users toward Chrome as a default browser. I believe there are better alternatives than the stock Safari and Chrome applications. I prefer Firefox Focus for all web browsing from within stock Apple or Android 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.
- **Simplicity and Speed:** I believe Firefox Focus offers the most simplistic and speedy web browsing experience out of all the popular options.

Additional Apps: As you proceed through the book, I present numerous technologies which apply to both desktop and mobile environments. As I do this, I provide recommendations for both Android and Apple systems. Overall, this is your device to personalize as you desire. Never let me or anyone else completely control the way your device is configured. Make sure you understand the reasons behind the recommendations and skip anything which does not apply to you and your usage.

Exit Strategy: I offer a final 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.

iOS Mobile Device Firewall

When you launch an application within your mobile device, several network connections are executed. By default, we do not know much about these transmissions. Obviously, communication apps need to connect to servers in order to function. However, what else is happening behind our backs? Is your favorite “privacy app” sending data to social networks without your consent? I was surprised to learn of the number of privacy violations occurring when popular applications where opened. This is the reason I rely on a firewall on all of my devices. Let’s start with the iPhone.

Lockdown (lockdownhq.com) is a simple firewall which is free and completely open-source. Installation from the App Store is easy, but the software is not activated upon installation. Enabling the firewall adds a virtual VPN configuration to your device. This connection intercepts all local network traffic and provides an option to block any undesired transmissions. Clicking on “Block List” reveals various collections of invasive tracking services which are commonly present within mobile applications. This includes tracking URLs from Facebook, marketing companies, and user trackers. My preference is to “Enable” every list. Next, it is time to test.

Open an application on your device, allow it to load, and close it. Open Lockdown and identify the blocked connections within the “View Log” option. This will disclose any suspicious traffic being blocked from that application to the tracking recipient. Repeat the process for each app on your device to discover any concerning activity. Anything you see in the log was blocked by the firewall. When an application attempts to send data to tracking companies such as Facebook, the transmission is blocked. You can also add any custom domain desired. I allow Lockdown to run at all times, and visit the log weekly to preview the content being restricted. The additional battery drain is minimal without any noticeable impact.

The business model of Lockdown is their paid VPN service visible within the firewall app. I find it to be overpriced and a bit “generic”, but I understand the need to make money on that service in order to keep the firewall free.

Many readers have discovered that running both Lockdown and a VPN application simultaneously can be troublesome. This is because Lockdown is acting as a VPN and conflicting with any other VPN service. The solution is to change the protocol of the VPN application. Within iOS, I launched the ProtonVPN application, opened the settings menu, and changed the protocol from OpenVPN to IKEv2. I could then launch the VPN application while Lockdown was running without any conflicts. You should be able to replicate this with other VPN providers if they offer this alternative protocol.

Android Mobile Device Firewall

Android (and GrapheneOS) users who want a similar firewall should consider **Blokada**. It is free, open-source, and does not require “rooting” in order to function. Always download the latest version, which was “5” at the time of writing. By default, the application is disabled, so be sure to toggle the top switch after installation. You may be asked to confirm several permissions, all of which are acceptable. After enabling the service, tap the “Advanced” button then tap “Blocklists”. This presents the various defined blocklists. Most users are protected with the default list (OISD), but I also enable “Developer Dan’s Hosts”. You may see a better option which matches the protection of Lockdown.

I also recommend **NetGuard** (netguard.me) for some users. This application allows you to specify any apps which should have no access to the internet. As an example, I have a music player installed which only plays local files stored on my device. It does not need to connect to the internet and I do not want it to send out any data. In order to prevent any incoming or outgoing connections, I could enable NetGuard for that app. This may be overkill for most users. If you limit the apps on your GrapheneOS device only to those used for vital communications, you likely have no need for NetGuard.

Note that you can only use either Blokada, NetGuard, or a VPN at any given time, and they cannot be used simultaneously. This is because they all rely on a traditional VPN connection. I believe Blokada is more valuable than NetGuard, but a VPN is more beneficial than both other options. If you are not using your GrapheneOS mobile device for web browsing or game playing, you probably do not need either Blokada or NetGuard. However, a VPN masks your true IP address and is more beneficial to privacy. When a client agrees to commit to a GrapheneOS device, I only include the ProtonVPN application and never Blokada or NetGuard. I mention these firewall apps as more of a cautionary tale than any endorsement.

Linux Phones

In 2020, I saw the emergence of two privacy-respecting Linux telephones from **Purism** (puri.sm) and **Pine64** (pine64.org). Both offer the ability to physically disable the cameras, microphones, and communications hardware. This alone is a huge feature for us. Both devices possess Linux operating systems which provide enhanced privacy and security. On the surface, these devices sound perfect. Unfortunately, this is not the case. Both devices rely on your cellular service provider for standard calls and communication. VOIP is possible, but extremely limited. Google Voice and MySudo will not work with these devices. Linphone is supported, but difficult to configure. At the time of this writing, Wire, Signal, ProtonMail, Tutanota, and CTemplar do not support the operating systems. This eliminates the vast majority of features I require in a mobile device. I truly hope that the future presents a scenario where a Linux phone meets all of my needs. Until then, I do not recommend these devices.

Camera and Microphone Blocking

Our mobile phones are designed to make life simple and fun. Most devices possess 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. The most recent iOS and Android operating systems possess protections from this type of misuse, but bad things can still happen.

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 camera and microphone blockers for the devices of all clients (and my own).

Camera blockers are easy. Much like a laptop, you can cover your mobile device cameras with black electrical tape or a dedicated sticker. Silent Pocket (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 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 iPhones possess 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 inline 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 inline 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 these earbuds, you would hear the other party, but they would not hear you. The device is only listening for the microphone plugged into the phone.

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. Figure 2.01 (left) displays one of these options, a standard 3.5mm microphone plug made by **Mic-Lock** (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 inline microphone. Therefore, it 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 used with GrapheneOS has a traditional headphone jack ready for these blockers. This is another benefit of the Pixel GrapheneOS strategy over devices which have eliminated the standard headphone port, such as any modern iPhone.

Many newer mobile devices present this problem. Most do not possess traditional headphone jacks, and only offer a Lightning or USB-C connection. You have a couple of options if you want to block default microphone access in these devices. If you already have an adapter for standard headphones, you could attach a microphone blocker to this adapter, and insert the other end of the adapter into your phone. This should work, but would need to be tested.

Alternatively, some microphone blocking companies are now creating plugs for these new connections. Mic-Lock offers a Lightning port to 3.5mm headphone port adapter with the in-line microphone disabled. Figure 2.01 (right) displays this device. You plug it into the phone and plug your earbuds into the adapter. The advantage with this unit is that you could wear headphones (with or without a microphone) and disable the default microphone at the same time. The disadvantage is that a long adapter sticks out when only desiring the microphone blocking element, as seen in Figure 2.01 (right).

There are numerous “L-Shaped” and miniature microphone blockers which are much smaller and fit flush to the device. 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.

Have you ever participated in a group FaceTime call or conference chat and accidentally pressed the option to activate your device camera? I know I have. Fortunately, my camera blocker stopped any video transmission to the other participants. Hopefully, you will never need to rely on the protection of a camera or microphone blocker. Proper protection eliminates threats and provides peace of mind.

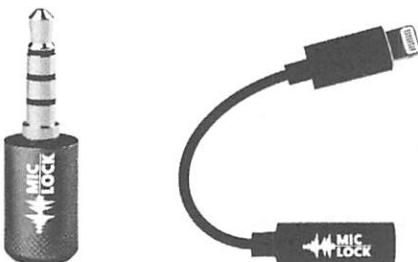


Figure 2.01: Microphone blocking devices.

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. If you are using an iPhone, tapping the network options on the home screen will not suffice. You must go to the Settings application and manually disable both Wi-Fi and Bluetooth. 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.

As stated previously, my travel phone never connects to any public Wi-Fi (or my home's network). I only rely on the cellular data package and I do not use my device for internet browsing or video streaming. It is a basic communications device and not an entertainment screen. This eliminates most privacy and security risks associated with mobile devices.

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 3.5mm stereo port available in most modern cars. If you have an iPhone, you will need a lightning to 3.5mm adapter, but Androids with a traditional headphone jack, like the Pixel with GrapheneOS, are ready for this connection natively. Once you have a device which is capable of this connection, rely on a standard 3.5mm male to male stereo audio cable without requiring any wireless signals or USB data connections. Please eliminate any technologies which makes you easier to track.

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 them 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 (explained later), 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.

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 free apps create a digital simulation of a cracked screen. These are not always convincing, but should work from a distance.

Pagers

I received my first pager in the mid-nineties. It was amazing. I could be anywhere, and receive a ten-digit number requesting a callback. This sounds archaic today, but the technology was fascinating at the time. This eventually led to alpha-numeric pagers which could deliver full text messages from standalone devices connected to a landline. This may seem unnecessary today, but the technology still exists and pagers are still available. The biggest consumer is the medical industry, where pagers work well when cellular signals cannot reach portions of hospitals. I have had only one client request a pager for daily use, but I know of a few people in my circles who continue to carry these devices. I will explain some extreme use cases that may encourage you to investigate further.

The benefit of pagers over cellular telephones is coverage and privacy. Your traditional mobile device is constantly communicating with multiple cellular towers, all of which are documenting your location. Contrary, pagers receive communications without sending an exact location back to the tower. The outgoing message is sent like a “blanket” over the entire coverage area. This also occurs on a much lower frequency, allowing the signals to reach further than a traditional cellular carrier. This is over-simplified, and I am not a pager frequency expert. Overall, pager companies do not know exactly where you are, but can still get messages to you wirelessly. There are three main types of pagers for our use, and each may have benefits and limitations for your needs. Each of these can possess various protocols for message delivery, and all have security weaknesses. It is common for network penetration testers to intercept pager messages.

- **Numeric:** I can call your pager number, enter a telephone number, your device notifies you of the number entered. I also have the option of leaving you a voicemail message which presents a notification in order to retrieve the message.
- **Alpha-numeric:** I can send you a text message via email, internet, or standalone unit. I can also replicate the features of a numeric pager.
- **Two-way:** You can receive messages via the previous options, and an attached keyboard on your device allows you to respond.

My client that desired a pager only required a numeric unit. He was an extremely high-risk target who did not carry a cellular telephone at all times. He subscribed to my Faraday bag usage and only removed his device when he needed to make a call. However, he had concerns about his children. The school was aware of threats made to the entire family, and had strict orders to contact my client if anything suspicious happened. The school possessed the number to his pager, and would leave a message when they needed to reach my client. His wife also had this number. If a voicemail was left on his account, he received notification of this almost instantly. I must confess that I do not possess or require a pager, nor do many people I meet. For those that need extreme privacy and security, it is a viable option.

Typical Client Configuration

There is a lot of information to digest here. In effort to minimize the decisions required to incorporate a private and secure mobile device into your privacy strategy, I present a common configuration for a typical client in need of extreme privacy.

- Purchase a Google Pixel 4a or newer with cash locally.
- Install and configure GrapheneOS on the Pixel device.
- Configure at least one VOIP number through Twilio or Telnyx.
- Install and configure F-Droid and Aurora Store on the device for app installations.
- Install and configure Linphone on the mobile device and laptop for traditional calls.
- Install and configure Signal on both mobile and laptop using the VOIP number.
- Install and configure Wire on both mobile and laptop.
- Install and configure the Mint Mobile app on the mobile device.
- Activate cellular service through Mint Mobile.
- Port any prior phone numbers to Google Voice.
- Forward any Google Voice calls to the VOIP number.
- Forward any Google Voice text messages to email.
- Install and configure ProtonVPN on the mobile device.
- Provide a Faraday bag, cam covers, and mic blockers for the device and explain usage.
- If desired, configure a secondary mobile device with an iPod Touch.
- Update the device apps via F-Droid and Aurora Store regularly.

Summary

Hopefully, you now possess a new phone with absolutely no public connection to you. It has service through a T-Mobile reseller which does not know your true identity. The service is paid through either prepaid cards or your Privacy.com account (explained later). The phone has never connected to any cell towers near your residence thanks to your new Faraday bag. There is no cellular location history associated with your home. Your secondary iPod Touch is the only mobile device used in your home and it possesses a unique Apple ID, while never leaving the house. Your old number forwards to Google Voice and eventually reaches both your primary and secondary devices. This all happens with zero knowledge from your cellular carrier.

All mobile telephones are tracking devices. We can never change that. When there is no association to your true identity, the threat of this tracking is minimized. There will always be a digital trail, but these tactics make you a very difficult target.

CHAPTER THREE

DIGITAL LIFE

I assume you now have a private and secure mobile device and computer. This provides a great backbone for secure and private digital activity, but we are far from ready to defend ourselves online. This chapter presents many considerations for extreme privacy and security on the internet. This may be the most important chapter in this book and is applicable globally. Most tactics presented here are completely free, and the others possess minimal cost. I hope you find a few ways to strengthen your online security.

Password Vulnerabilities

In 2018, I had a client that 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”. It was easy for her assailant to access her accounts. He knew the main word in her password because of data breaches.

There are thousands of breached databases floating around online, and you are likely in one or more of them. 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.

For our purpose, it will not matter whether you are exposed. Assume that all of your passwords have been compromised. During an initial visit with a client, I determine the important sites which will need to be accessed, and begin the process of changing every password in his or her digital life. This will require a password manager.

This is where I try desperately to avoid a debate about which password manager is best. Simply choosing a side of offline or online managers is likely to cause a dispute quickly. Remember, we want extreme privacy and security. Therefore, all of my clients in immediate danger transition to an offline password manager, specifically KeePassXC.

Password Managers

KeePassXC is an open-source password manager that does not synchronize content to the internet. There are many convenient online password managers that are secure and keep all of your devices ready for automated logins. Those are great for entry-level security, and millions of people are safely using them. It is not enough for our needs. Furthermore, I believe that my clients should choose an individual machine for sensitive account access, eliminating the need for synchronization between devices.

My clients all receive a tutorial on KeePassXC. KeePassXC is cross-platform and free. It will work identically on Mac, Windows, or Linux. Download the software from the official website at keepassxc.org, or install into Ubuntu via Terminal with “`sudo snap install keepassxc`”. 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 50 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 that you do not know. I encourage clients to write it down in a safe place 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, make a copy of the file on an encrypted USB drive. I will explain more about this later, but 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.

Personally, I keep my KeePassXC database within an encrypted VeraCrypt container (explained later) within a laptop drive with full-disk encryption. I then backup this entire drive to an external hard drive with full-disk encryption. This external drive is left with a trusted friend who could ship it to me if ever needed. Without knowing the passwords to the encrypted drive, VeraCrypt container, and KeePassXC database (all unique), this drive is useless. These three passwords are the only passwords in my life I keep in my memory.

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/) or Chrome 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 don't want a machine doing this for me. However, many clients insist on having this convenience. Therefore, let's walk through the process.

- Once you have KeePassXC installed, configured, and in possession of your passwords, install the KeePassXC Browser extension into the browser of your choice (I prefer 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 recommend **Strongbox** (strongboxsafe.com) for iPhones and **Keepass2Android Offline** (F-Droid) for Android, including GrapheneOS.

Strongbox 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. There are two big advantages to this scenario. Obviously, you have the convenience of passwords being present on 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. 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.

If using a Windows device, you could install iTunes and import the database through that software. You could also transmit the file securely to yourself through encrypted email and download the file within your mobile device, but that is outside of my comfort zone due to it touching the internet.

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. Changes made to your primary database on your laptop will not be applied to this mobile version. You would need to replace the mobile version with a new copy on occasion. 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. They should only make changes on that primary database, and consider the iOS 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.

GrapheneOS users can simply connect their devices via USB to any Linux or Windows computer and copy the database onto the phone. You can then open the Keepass2Android Offline app and browse to the file. If desired, you can configure the Pixel fingerprint reader to unlock the database upon opening.

Again, I want to stress that browser extensions and mobile solutions are optional. In a perfect scenario, you do not need access to your passwords on a mobile device or within automated browser extensions. Only you can decide the balance of security versus convenience which is best for you. If these conveniences are required to ensure you use a password manager for all of your accounts, I believe they are justified. If you can get by without them, even better. The attraction to online password managers such as Lastpass and Dashlane is the ability to sync the password database to all devices over the internet without manual interaction. I understand the benefits of these features, but it also comes with risk. All reputable online password managers encrypt the passwords locally on the user’s device before syncing with their own servers. Theoretically, no one at the password manager company would have the ability to see your individual passwords. However, nothing is hack-proof. It is only a matter of time before something goes wrong.

By keeping your passwords in an offline database such as KeePassXC, you eliminate this entire attack surface. However, I respect that some clients do not want to apply the time and effort of maintaining a secure password database locally. If you insist on using a cloud-based password manager, I highly recommend **Bitwarden** (bitwarden.com). Bitwarden is open source software with all of their source code free for anyone to review. They have been audited

by reputable third-party security auditing firms as well as independent security researchers. While nothing is bullet-proof, I believe this is the most secure option for an internet-based solution. Bitwarden does not store your passwords in plain text. It stores encrypted versions of your passwords that only you can unlock with your master password. Your information is encrypted locally on your device before being sent to their cloud servers. Most of my clients rely on the free version of this product, but advanced users may require a paid tier. Installing the Bitwarden application on all of your devices simplifies the synchronization of your database. It eliminates the headaches of manual updates.

Creating and storing secure passwords through Bitwarden, or any other online service, should be similar to other password managers, such as KeePassXC. Due to constant user interface updates, I will not present detailed usage instructions. It is vital that you feel comfortable with the application you choose, and that you understand how to update and save any changes.

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, the following steps will download an offline copy of your passwords.

- Log in to your web vault at <https://vault.bitwarden.com>.
- Click “Tools” in the top navigation bar.
- Click “Export Vault” under the side navigation.
- Choose a file format, type in your master password, and click “Export Vault”.

I recommend placing your backup within your VeraCrypt protected container, as explained momentarily. In the worst-case scenario, you could import this backup into another password manager solution and have the ability to access all of your accounts. I have had three clients who lost access to their passwords through their online password managers and had to attempt password resets through every account. A backup would have prevented this frustration.

Again, I do not use cloud-based password managers, and I encourage my clients to avoid them, but I respect those who require this level of convenience. 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 your primary email addresses and any online calendars. 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.

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 cell phone number). It is vital to enable 2FA anywhere 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 preferences, in order, are the following.

Hardware Token: I use a **YubiKey** (amzn.to/2HZlT0Z) daily. This small device which plugs into my USB port is required before I can access my business 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 provides me access to the service. Without the presence of this physical USB device, I cannot gain access 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.

Software Token: If a service does not support a hardware token, then I prefer using **Authy** (authy.com) as my software-based 2FA. I choose Authy over amazing open-source options such as **Aegis** (getaegis.app) because it is much easier on my clients (and myself). I have learned that making anything overly complicated will result in lack of use. I do believe that other options are possibly more private on an extreme level, but they are more difficult to use on multiple devices. Authy works on Linux, macOS, Windows, iOS, and Android, and you can use a temporary code from any device at any time. At the time of this writing, the Linux version was still in beta, and could be installed via Terminal with “`sudo snap install --beta authy`”. GrapheneOS users can install through Aurora Store. I download Authy to all mobile and desktop devices then create a new account through the mobile application. Under “Devices”, enable “Allow Multi-Device”, then open the desktop Authy app and follow instructions to connect to an account. Once you successfully have Authy working on all devices, disable “Multi-Device”.

You can now add any services to your Authy account which allows a software-based 2FA. I use Authy to protect my ProtonMail account. Opening Authy on any of my devices presents a new code every thirty seconds. After providing my username and password to ProtonMail, I am prompted for this temporary code. Entering that code completes the login process. Without it, I am locked out of my account (and so is anyone else who might obtain my password). You can visit <https://authy.com/guides> for details about the most popular services. I use it with Amazon, my web host, and numerous additional accounts.

My only gripe with Authy is that it requires a telephone number in order to associate your account across multiple devices. Always use your VOIP number previously created. The benefit of this requirement is that you can regain control of your account in the event of broken devices. Since VOIP numbers are allowed, I do not see a huge privacy invasion compared to benefit. Make sure you provide a number which you will own long-term.

SMS Token: If an online service you use only supports 2FA via a text message, it should still be used. While not optimal, it is better than no protection at all. I never recommend using your cellular number provided by your carrier, as it is prone to SIM swapping attacks. Instead, I use Google Voice. This may seem surprising due to my criticism of Google's privacy policies, but their security is top-notch. Their Google Voice service is free and can be protected by a hardware token, such as a YubiKey. Once you have a Google Voice account created using the previous instruction, you can provide your Google Voice number whenever required for SMS 2FA. If you enabled the email forwarding protocol, those codes will appear in your inbox. If you adopted the Linphone strategy, you could also use your new VOIP number. However, you may encounter issues with short codes being blocked. This is why I prefer Google Voice.

Be sure to secure the Google account with a hardware or software token, preferably a YubiKey. Some readers of the previous edition of this book expressed concern over the ability of companies to track us through use of a single hardware token (YubiKey) across multiple accounts. This is a valid concern if you are using the One Time Password (OTP) option of YubiKey, but not a big concern if using the more secure Universal 2nd Factor (U2F) option. I will explain each.

OTP provides a unique code every time you touch your YubiKey. You can test this while within a text processing application. Every time you activate the YubiKey, a new line of data is entered. However, the first 12 characters are always the same and represent the serial number of the YubiKey. This is concerning, as it could associate two accounts with the same device; therefore, associating multiple accounts to the same individual (you). It could also leak your YubiKey serial number upon accidental touch during a text conversation or make you slightly more prone to a phishing attack when someone attempts to steal a valid token in order to access your account. However, most sites do not use OTP today. If they do, they also offer a U2F option.

U2F creates a unique challenge and response each time it is configured for an account. There is no static line of text which can be misused. Google, Twitter, and others offer hardware token service through U2F only. Therefore, using the same YubiKey within multiple Google accounts does not clearly connect them to each other. Always look for a U2F option when registering a YubiKey with a service. If no clear protocol is identified, do your research.

“Proactive” Two-Factor Authentication (2FA)

In 2021, I witnessed numerous online services automatically enrolling customers into 2FA. On the surface, this sounds like a great idea. However, the execution can actually harm our privacy strategies. This is where I consider “proactively” initiating 2FA before a company forces you to use a cellular telephone number as part of your login process. Consider the following experiences from myself and my clients.

A client logged in to her PayPal account with the correct username and password. She was prompted to enter a six-digit code which would be sent to her cell number. She had never provided a cell number within her account, so PayPal demanded a number be added before she could access the account. PayPal would not accept a VOIP or landline number. She had no way to access the account until she had provided a true cellular number to be used for 2FA. If she had added 2FA through a software program such as Authy, she would not have been prompted to enter a cellular number in order to complete the login process.

Another client found herself locked out of her online banking. After successfully providing her credentials, the bank demanded a cellular number for a one-time confirmation code to verify her identity. Due to her usage of a VPN, the bank found this login attempt suspicious and wanted an additional layer of confirmation. Similar to PayPal, she was not allowed to enter a VOIP or landline number. She was forced to enter her true cellular number in order to access her funds. If she had implemented any form of 2FA before this login, she could have used that for the confirmation and avoided disclosure of her cellular number.

I conduct a lot of online investigations which requires me to maintain hundreds of alias social network profiles. Many of these do not get used often. When I log in to an account after it has been dormant for several months, I am often asked to provide an additional form of identity confirmation. If 2FA is activated on the profile, I rarely see these demands and I can simply enter a temporary software token. This is why I configure 2FA on any social network profile immediately after account creation. It prevents me from losing access to the account due to demands for a valid cellular number.

In summary, I encourage you to activate 2FA on every online account which supports it. This may prevent many headaches and also secures the account from intruders. ANY 2FA is better than NO 2FA. Practically every “hacking” scenario which happens to a client could have been prevented by using 2FA. Hardcore privacy and security enthusiasts should look into the OnlyKey, which is explained in a moment. While I use one, I have yet to have a client commit.

Advanced Hardware Two-Factor Authentication (2FA)

Previously, I explained the usage of a hardware token as part of a Two-Factor Authentication (2FA) strategy, such as the YubiKey, in order to protect your online accounts. In that writing, I explained the benefits of U2F over traditional OTP, both of which are provided by the USB YubiKey device. In this section, we will take things to another level. First let's revisit the best practices for a YubiKey, and I will demonstrate with a new Fastmail account created specifically for this explanation.

After logging in to the account, I navigated to Settings > Password & Security > Two-Step Verification > Add Verification Device. This allowed me to choose to use an authenticator app (such as Authy), U2F through a hardware token, or OTP with an older YubiKey. Since U2F is the most secure option, I chose that. Fastmail walked me through the steps to activate my YubiKey for their service. Now, any time I log in to Fastmail, I am prompted to touch my flashing YubiKey in order to complete the process. This prevents remote access to my email, even with a known password. I replicated the process to associate this YubiKey with test Gmail and Twitter accounts. Both used U2F by default. My YubiKey is now required for all of these accounts. However, there are additional features available to us through the YubiKey.

YubiKeys possess two virtual “slots” which can store small amounts of data. These slots can be used to facilitate a One-Time Passcode (OTP), static password, challenge-response credential, or OATH credential. By default, the first slot is designated for OTP. Since I do not use any services which rely on OTP (because I always use U2F), I can modify both of these slots. For the first slot, I will add a static password. In order to do this, we must download the free YubiKey Manager application, available for Windows, Mac, and Linux, from their website at <https://www.yubico.com/products/services-software/download/yubikey-manager>. After installation and launch, I conducted the following steps.

- Click on “Applications” and then “OTP”.
- Under “Short Touch (Slot One)”, click “Delete” and confirm.
- Under “Short Touch (Slot One)”, click “Configure”.
- Select “Static Password” and click “Next”.
- Click “Generate” and click “Finish”.

Your YubiKey now possesses a long and secure password in the first virtual slot. Any time you touch the device, it will type in this static password into any active window. The password never changes. This is not any type of 2FA, it is merely a convenience. This static password could be used to strengthen account security, especially when associated with a desktop application. Consider the following examples, assuming that my static YubiKey password is RkDNTRggchNceYTknLBjDNiNrJrhcFvjbRCHrt (my actual test password).

Secure Messaging: When I open Wire on my Desktop, I must provide a password. Since I insist on my passwords being lengthy and secure, I must either manually type in the credential or copy and paste one from my password manager (KeePassXC). Alternatively, I could make the password for Wire RkDNTRggchNceYTknLBjDNiNrJrhcFvjbRCHrt and simply tap my YubiKey each time I need to log in. While convenient, this does pose some risk. If anyone possessed my YubiKey, the password could be entered without my input or any knowledge of the credential. Therefore, I always add unique characters before the password. My password could be wire!4RkDNTRggchNceYTknLBjDNiNrJrhcFvjbRCHrt. In other words, I could type wire!4 and then tap and hold the YubiKey. This would allow me to continue using this static password with other applications and services without replicating the exact same password everywhere. Overall, this is more convenience than security, but it can add password complexity in various scenarios. I would never recommend this for all your online accounts. I bring up Wire because it is an application which I open many times every day. In order to access my account, you would need to know my username, my added characters (wire!4) and my long YubiKey static password. If you have an application which requires constant input throughout the day, this could be a useful strategy. Be sure to store your static password within your password manager in case you lose or break the YubiKey.

Operating Systems: I use many computers throughout a typical day. I have my primary Linux laptop, a MacBook Pro for production purposes, a media center, a firewall, and other various devices. Let's focus on my media server. There is nothing overly sensitive present, but I do insist on a strong password and an encrypted drive. When booting this computer, it boots to Ubuntu Linux and prompts for a password. I do not have a physical keyboard or mouse attached to this unit, and the monitor is my television. Since I leave my YubiKey attached to my primary keyring, it is always with me. I simply plug the YubiKey into the front USB slot of the media center, touch the YubiKey, and my lengthy password is entered. The computer finishes the boot process and launches Kodi, which allows me to stream all of my audio and video. I do not recommend this strategy for personal computers containing sensitive information. If someone stole your YubiKey and laptop, he or she would have everything needed to log in. I only recommend this for household devices which are not extremely sensitive.

Encrypted Containers: As I mentioned previously, I possess a VeraCrypt container which contains my KeePassXC database. In order to open the container, I must know the password. Since I cannot open my password manager without first opening the container, I cannot store my container password inside KeePassXC. Therefore, I must remember the password to the VeraCrypt container. Assume my memorized password is VC!76T84R911. That might be easy for me to remember, but it is not very complex. It is not obviously a VeraCrypt password, but it could use more characters. I could make my password to VeraCrypt extremely strong by using VC!76T84R911RkDNTRggchNceYTknLBjDNiNrJrhcFvjbRCHrt. I would then type VC!76T84R911 into the VeraCrypt password field and then touch my YubiKey.

Now that I have explained some uses for static passwords stored within a YubiKey slot, let's consider a "challenge-response" option for our KeePassXC database. Currently, you may have a secure password memorized for your KeePassXC password manager. You may want to add a layer of security to that strategy. After all, your password manager likely stores access to all your accounts. Open the YubiKey Management application, and conduct the following.

- Click on "Applications" and then "OTP".
- Under "Long Touch (Slot Two)", click "Delete" and confirm.
- Under "Long Touch (Slot Two)", click "Configure".
- Select "Challenge-response" and click "Next".
- Click "Generate" or create your own randomly generated secret key.
- Enable the "Require touch" option.
- Click "Finish".

The second slot of your YubiKey is now configured for a challenge and response. Launch KeePassXC and open your password database. To be safe, you may want to make a copy until you have tested your final project. I save a copy any time I make security changes to a database. You can now enable this challenge and response feature within your password manager. Conduct the following.

- Click "Database" in the file menu and choose "Change Master Key".
- Click "Add additional protection".
- Click "Add YubiKey Challenge-response".
- Ensure the application detects the YubiKey and click "OK".
- When prompted, touch the flashing YubiKey.
- Close the database and application completely, then reopen KeePassXC.
- Input the password, select the YubiKey in the "Hardware Key" field, and click "OK".
- When prompted, touch your flashing YubiKey.

You have now added an additional layer of security to your password manager. Every time you log in to the database, you will be required to insert your YubiKey and touch it. If you prefer, you could make this second slot another static password instead of a challenge and response. If you choose this route, a short press of the YubiKey will type the first static password while a long press of two seconds will present the second static password. Personally, I prefer the challenge and response availability. Since YubiKey allows only two slots, we have reached maximum capacity for our device. However, this is where the **OnlyKey** (amzn.to/2CVUF7l) enters our password strategy. This device applies the same benefits of the YubiKey, but provides 24 virtual slots.

OnlyKey

The OnlyKey device is similar in size to the standard USB YubiKey hardware token. I prefer the YubiKey Nano device for daily use, as they sit practically flush with either a USB-A or USB-C port. However, the OnlyKey is much more powerful, and is always on my key ring. This device requires the OnlyKey application on a computer in order to easily program a PIN and customize complete function, but can be used on any computer without the software after it is configured. Therefore, let's install the application and configure the device. A current online guide is always available at docs.crp.to/usersguide.html.

- Navigate to the above website and download the OnlyKey app for your OS.
- Install the app with default options.
- Launch the app and click the “Guided setup” button.
- When prompted, choose and enter a PIN to protect the first 12 slots.
- When prompted, choose and enter a different PIN to protect the second 12 slots.
- When prompted, if desired, enter a self-destruct PIN.

When complete, your OnlyKey is now ready for use. When you insert it into a USB slot, you must enter the PIN assigned to either bank one or bank two before it can be used. After you have unlocked the bank, you can use it as a U2F device right away. You would set it up the same as the previous instructions for the YubiKey. Pressing any button (1-6) confirms the response as a U2F device. The power of the OnlyKey is the 24 slots which can be programmed with URLs, usernames, and passwords. Figure 3.01 displays the OnlyKey application.

After you have inserted the OnlyKey, opened the OnlyKey app, and entered the PIN for either bank one or two, you are ready to customize a slot. I conducted the following on a new OnlyKey which contained no prior programming. This example allows me to navigate to Twitter, enter a username, enter a password, execute the login, and apply U2F as a second factor of authentication.

- Click the button for the desired slot, for example “1a”.
- Enter “Twitter” as a label.
- Provide a URL of “<https://twitter.com/>”.
- Enter a delay of “2”.
- Enter the Twitter username.
- Enable “Tab after UserName”.
- Enter the account password and confirm.
- Click “Set slot”.

I can now open a new browser tab and tap the “1” button on the OnlyKey and the device will go to Twitter and log me in. If I had set up U2F on the account, the OnlyKey would blink in order for a second tap (after login) which would complete the 2FA login. I can repeat this process to store up to 12 logins for each bank. Each button (1-6) has two options. Option “a” requires a single short tap of the button while option “b” requires a touch and hold of two seconds. You can also choose to store only a password if desired. Before you configure your credentials for 24 sites, we should discuss any security risks from these actions.

The availability of all needed credentials within a single hardware device is enticing and convenient. It also can be reckless. If I steal your OnlyKey and know your PIN, I have everything I need to log in to any accounts represented on the device. This is a scary, even if rare, possibility. I do not use the OnlyKey this way. Instead, I rely on it to strengthen other passwords, similar to the options presented earlier. The following is a fictional example of my OnlyKey slots based on my real usage.

- | | |
|---|--|
| 1: Entire password to media center login | 13: Last 20 characters of MacBook login |
| 2: Entire password to media center FTP | 14: Last 20 characters of Apple password |
| 3: Last 20 characters of email password | 15: Last 20 characters of Linux login |
| 4: Last 20 characters of Wire password | 16: Full credentials to Wi-Fi router |
| 5: Last 20 characters of Authy password | 17: Password to unlock this book in Word |
| 6: Last 20 characters of Notes password | 18: Password to unlock my OSINT book |
| 7: Session app ID 1 (to send to contacts) | 19: Terminal command |
| 8: Session app ID 2 (to send to contacts) | 20: Terminal command |
| 9: Forum URL, user, and password | 21: GVoice URL, user, password, & 2FA |
| 10: Twitter URL, user, password, & 2FA | 22: GVoice URL, user, password, & 2FA |
| 11: GVoice URL, user, password, & 2FA | 23: GVoice URL, user, password, & 2FA |
| 12: Amazon URL, user, and password | 24: GVoice URL, user, password, & 2FA |

I present these storage options to give some ideas for your own configuration. Often, I use the OnlyKey to easily generate complicated text. As an example, I use Session as a secure messaging option with some clients. It relies on a randomly generated “Session ID” which is used in place of a username. I need to send this information to clients, usually via email. I could never remember this long string of random characters, but it is only a button press away. Some services which are used as “burner” accounts, such as Google Voice, are not vital to keep extra secure. Storing the URL, username, and password for these accounts allows me to quickly and easily log in to the service. If I am expecting an incoming Google Voice call, I can press one button and be ready to answer in seconds versus opening my VeraCrypt container, providing a password, opening KeePassXC, providing a password, copying the Google username, pasting into the website, copying the password, entering into the website, and executing the login. Hopefully you now see the benefits of an OnlyKey. Figure 3.01 displays the OnlyKey application which identifies my configuration for the first 12 slots.

Now that you have configured your OnlyKey device, you should make a backup of the data. If you lose the device, or need to reformat for any reason, you can replicate your hard work easily. Personally, I keep a clone of my OnlyKey in a safe place for emergency usage. The following steps generate a backup file which can be imported into any additional OnlyKey.

- Launch the OnlyKey app, insert the device, and enter your PIN for the first bank.
- Click “Setup” and then “Set Backup Passphrase or Key”.
- Click “Save passphrase or key” and document it in your password manager.
- Click “Backup/Restore” and click within the text box.
- Hold the “1” button on the device for at least five seconds.
- Allow the backup text to populate the input box.
- Click “Save file” and store the backup file safely.
- Repeat for the second bank of slots.

There are many additional benefits of the OnlyKey, and I have only focused on the most common features. Unlike the YubiKey, OnlyKey requires you to unlock the device when inserted into a USB port. This prevents a stolen device from being used without your consent. If the wrong PIN is entered ten times, the device wipes itself as a precaution. The device is not a threat if stolen or seized. I encourage you to visit docs.crp.to/usersguide.html and explore other possibilities.

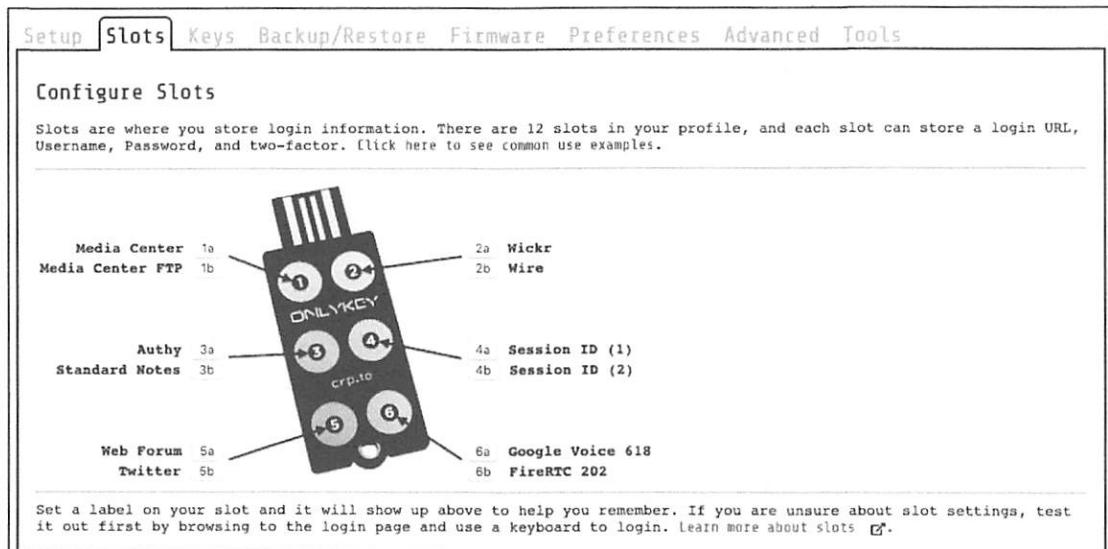


Figure 3.01: The OnlyKey application displaying configuration.

Encrypted Storage & Backup

I mentioned encryption earlier, and it has been a popular hype word over the past few years. Encryption can mean many things, depending on how it is applied. Previously, we applied full-disk encryption to the entire drive of the computer. In this section, it refers to software encryption on a physical device, such as a USB drive. This works by automatically converting data on a drive into a form that cannot be understood by anyone who doesn't have the password to reverse the conversion. Without the proper password, the data remains inaccessible. This is extremely important in case you lose a device, especially a portable drive used as a backup. If I steal your USB device, and you did not apply encryption, I can access all of your files without the password to log in. If you encrypted your data, I cannot extract anything. I apply the following backup and encryption practices for the removable devices.

I first choose a backup device appropriate for the situation. For most clients, I choose a SanDisk Ultra Fit USB drive. These can be easily found in 64GB, 128GB, and 256GB options, and I choose the largest possible. These are small and reliable. I then install VeraCrypt (veracrypt.fr) on the computer. The download for Mac and Windows is easy to install, but Linux requires a few extra steps. Enter the following commands within Terminal in Ubuntu.

- sudo add-apt-repository ppa:unit193/encryption
- sudo apt update
- sudo apt install -y veracrypt

We can now begin the process of creating an encrypted container for our data.

- Click “Volumes” > “Create New Volume” > “Create an Encrypted File Container”.
- Choose “Standard VeraCrypt volume”.
- Click “Select File”, choose a name such as “Backup”, and select your USB device.
- Click “Save” > “Next” > “Next”.
- Enter the volume size lower than the specified limit (round down to nearest number).
- Choose a strong password for this container and click “Next” > “Next” > “Next”.
- Move your cursor randomly as the pool completes. When finished, click “Format”.

You now possess an encrypted container on a USB device. You can store anything within this container once it is mounted. To do this, open VeraCrypt, click Select File, choose the “Backup” file on the USB, select “Mount”, enter the password, and you should see that container as a new drive on your computer. Now that the device possesses an encrypted container ready for storage, we need to establish a backup solution. I prefer an open source solution rather than proprietary offerings from Apple or Microsoft. For my clients, I recommend **Free File Sync** (freefilesync.org). This site possesses free tutorial videos which

demonstrate usage better than I can explain in a couple of paragraphs. Always understand your backup solution before relying on it. The vital lesson here is that you should have a backup strategy which involves encrypted data. Backup anything important often, and only backup to an encrypted drive. If, or more likely when, this USB device is lost or stolen, you will not panic. The content can never be visible without your password. If your primary computer suffers a hard drive crash, you have a backup to restore the data. I am extreme on my own backup solution, and whenever I have a highly-targeted client, which I explain next.

First, my computer possesses full-disk encryption. Within that drive, I possess a VeraCrypt encrypted container 128GB in size. Within that container is everything important to me including photos, videos, documents, business data, and even my password manager. You must know the computer password and the VeraCrypt password to see anything. I possess a 128GB USB drive with full-disk encryption. It then contains a 127GB VeraCrypt container. I use Free File Sync to occasionally backup the content of the container on my computer to the content of the container on my USB drive. I then replicate this process with an additional external media which is stored off-site in case of true emergency. Is this overkill? Maybe. I would rather be safe than sorry. My clients store sensitive information which would be very valuable in the wrong hands. I take every precaution I can.

In 2019, I was forced to test my encryption and backup strategy during a series of unfortunate events. I had recently updated my password manager, KeePassXC. This new version possessed a bug in the code which would delete the database if stored on a Mac computer but inside another operating system file structure. Since my KeePassXC database was stored within a VeraCrypt container on my MacBook Pro, I was part of a small minority of users who experienced this flaw (this problem was patched a few days later by KeePassXC). When I closed KeePassXC, the database was completely deleted without any possibility of recovery. There was no warning, and I was unaware of the issue. When I conducted a daily backup of all data to my USB drive, it removed the copy of the KeePassXC database on it and replaced it with an empty folder. I now had absolutely no copy of my KeePassXC database, which was a catastrophe. When I opened my password manager, there was no option to see my passwords. After a brief moment of panic, I reached out to a friend who could help.

In my previous example of how I store my data, I mentioned an off-site external media which possessed a duplicate copy of all vital data. This is in the form of a 1GB micro SD card which contains a single 1GB VeraCrypt container. The password to open this container is unique from anything else, and I have it memorized. Without this password, the data is useless to anyone who takes possession of the card. This card was placed inside of a “hollow nickel” and stored secretly inside the home of a friend and former colleague. This is a real U.S. nickel which is made from two unique coins. Each coin is die-cut in order to create a top piece (heads) which fits into the bottom piece (tails) and allows for a hollow space in between, large enough to store a micro SD card, as seen in Figure 3.02. These cost approximately \$20-\$25.

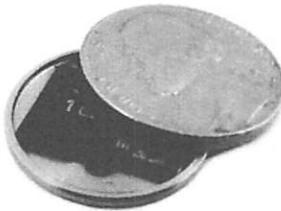


Figure 3.02: A hollow nickel with a micro SD card stored inside.

I called my friend and told him I was in a serious situation, and I needed his help without asking many questions. This person works in the intelligence community, so the request was well-received. I advised him to go into his upstairs bathroom and remove the power receptacle cover next to the mirror. He would then notice a nickel resting on the bottom of the outlet box within the wall. Remove that nickel and tap the edge of it on the bathroom sink. The top of the nickel will come loose and can be removed, revealing an SD card. The SD card should be inserted into a computer and the 1GB file should be uploaded to my own web server in a specific directory.

My friend agreed and completed each step. I then asked him to place everything back where it was, and that I would further explain everything over a beer the next time I was in town. Whenever I visit my friend's home, I update the contents of this drive without anyone's knowledge. It is much smaller than my other backup, but only contains the absolutely necessary data I would need in case of an emergency. This includes a current copy of my password manager, client documents, business files, and scanned copies of any identification I may need while abroad. I chose this friend carefully, as I know he is home often, he is extremely trustworthy, and he respects my extreme privacy antics. Hopefully you have someone similar in your life.

After he uploaded the 1GB VeraCrypt file, I was able to open it and destroy the online copy. I then had access to my password manager and could now access my passwords. This version of the database had not been updated in a few months, so I was still missing some recently changed passwords, but my email archive identified those accounts quickly. I was relieved to have my accounts back, as many of them date back over ten years.

I hope this serves as a reminder to the importance of an offline backup away from your home. If I ever find myself overseas with a lost passport, my friend can give me the data I need to obtain a new copy. If my hotel is burglarized and all of my data is stolen, my friend can get the essentials to me. I also maintain a hollow nickel near my home which contains a 128GB card with a full backup of all data. It takes me at least 20 minutes to retrieve it from my property. If someone can find my home, locate this nickel, open it to reveal the card, and beat the encryption, I deserve to be hacked.

Web Browser Configuration

Before we consider connecting to various websites in order to harden our accounts, we should configure a secure web browser. I recommend, and solely use, the Firefox web browser at all times. Your new Apple computer has its own browser called Safari, but I rarely touch it. Windows possesses Microsoft Edge, which I have not opened in several years. The only time I would consider using these options is to connect to www.mozilla.org/firefox and download Firefox. Once Firefox is installed and configured, I hide any references to Edge or Safari on my clients' machines. Installation of Firefox is easy and guided, and you can accept all default options. It is included within Ubuntu as the default browser. Once installed, execute the application and consider the following modifications.

- Click on the menu in the upper right and select “Options” 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 own sites in new tabs.
- In the Search options, change the default search engine to DuckDuckGo and uncheck the “Provide search suggestions” box. This prevents queries from going directly to Google, and blocks the Google API from offering search suggestions.
- 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 and generate strong passwords”.
- Uncheck the box titled “Autofill logins and passwords”.
- Uncheck the box titled “Ask to save logins and passwords for websites”.
- Change the History setting to “Firefox will use custom settings for history”.
- Uncheck the boxes “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.
- Uncheck “Browsing history” from the “Address Bar” menu.
- In the Permissions menu, click “Settings” next to Location, Camera, Microphone, and Notifications. Check the box titled “Block new requests...” on each of these options.
- Uncheck all options under “Firefox Data Collection and Use”.
- 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”.

Firefox allows users to modify many configuration settings, and some of these deal with privacy and security concerns. Though some of these changes can be made in the menu of Firefox's preferences, changes made through about:config tend to be more durable and granular. To access the list of configuration settings, open Firefox and type "about:config" into the URL bar. You will receive a warning about making changes within this area, but the modifications we make will be safe. Choose to accept the risks. Some of these about:config settings may already be on the "correct" setting, but most probably will not. To change most of these settings you can simply double-click the setting to toggle it between "True" and "False". Some may require additional input, such as a number. Because the list of about:config settings contains hundreds of entries, you will probably wish to search for all of these through the search bar in the about:config interface.

- geo.enabled: FALSE: This disables Firefox from sharing your location.
- browser.safebrowsing.malware.enabled: FALSE: This disables Google's ability to monitor your web traffic for malware, storing the sites you visit.
- dom.battery.enabled: FALSE: This setting blocks sending battery level information.
- extensions.pocket.enabled: FALSE: This disables the proprietary Pocket service.
- browser.newtabpage.activity-stream.section.highlights.includePocket: FALSE
- browser.newtabpage.activity-stream.feeds.telemetry: FALSE: Disables Telemetry.
- browser.ping-centre.telemetry: FALSE: Disables Telemetry.
- toolkit.telemetry.server: (Delete URL): Disables Telemetry.
- toolkit.telemetry.unified: FALSE: Disables Telemetry.
- media.autoplay.default: 5: Disables audio and video from playing automatically.
- dom.webnotifications.enabled: FALSE: Disables embedded notifications.
- privacy.resistFingerprinting: TRUE: Disables some fingerprinting.
- webgl.disabled: TRUE: Disables some fingerprinting.
- network.http.sendRefererHeader: 0: Disables referring website notifications.
- identity.fxaccounts.enabled: FALSE: Disables any embedded Firefox accounts.

WebRTC: These settings address a potential vulnerability of leaked IP addresses. If you use audio or video communications within your browser, these could break those services.

- media.peerconnection.enabled: FALSE
- media.peerconnection.turn.disable: TRUE
- media.peerconnection.use_document_iceservers: FALSE
- media.peerconnection.video.enabled: FALSE
- media.navigator.enabled: FALSE

It is not vital that all of these security settings be applied to your systems. Firefox natively respects your privacy and security more than other browsers. These recommendations are for those that want to tweak additional settings that may provide a layer of protection, even if minimal. 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 but experimenting with the advanced settings should help you understand the functionality. 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 addons.mozilla.org/en-US/firefox/addon/ublock-origin/. 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. 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". Click on the Filter lists tab and click the "Update Now" button at the top of the page. This will refresh all of the data and apply your new settings. You now have extended protection that 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. This protection will suffice for most users, but dedicated privacy enthusiasts may choose to take a more advanced approach.

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 by loading the website cnn.com. Within the uBlock Origin menu while viewing cnn.com, you will see all scripts that have either been loaded or blocked. You may see several questionable scripts such as "Twitter-ads". 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. 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.

Using this same page, let's modify the options. Click 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 (upper left "padlock"). 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 reversed my actions by clicking on the left 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 original site.

Next, we will modify the second (middle) column, which will apply the settings globally. By default, all options are grey in color. This indicates that the default block list is applicable, and only invasive scripts will be blocked everywhere. Click on the far-right portion of the top cell in the second column. This turns the entire column red, and indicates that all scripts across all websites will be blocked. After saving changes, every website will only load the most basic text content. This will break practically every website.

Loading a page such as a Twitter profile results in no usable content. By clicking on the uBlock Origin icon and clicking the left sections of specific cells within the third column, you can enable those scripts without allowing everything on the page. 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](#), [twimg.com](#), and others are grey. Those scripts will be allowed, if approved by uBlock Origin's rules, only for that domain. If you loaded a blog that has scripts from Twitter, they would still be ignored.

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. Know that you have great protection against most invasions. Before you navigate to a questionable site that may try to install malicious code on your machine, click on the far-right section of the top cell in the second column. That will block all scripts on all pages. Conduct your internet usage, enabling any desired scripts as needed on the questionable page, and reverse the changes when you are finished. Remember to click the save button (padlock) after each change.

I also use this plugin to bypass website restrictions. As an example, consider my local newspaper, The Chicago Tribune. When you navigate to chicagotribune.com, you are allowed to view three articles before being blocked with a message which states “You’ve reached your monthly free article limit. To continue reading, subscribe now”. Clicking any further articles blocks your access. You may have seen similar messages from websites when using any type of ad blocker. Clicking the uBlock Origin icon reveals it is blocking 14 scripts, but something is still running in order to know the number of articles I have read. Choosing the far-right option (red) within the line titled “Inline scripts” blocks these types of annoyances from this domain. Clicking the lock (save) option and reloading the page eliminates the barrier permanently. It also makes the page load much faster. I can now browse this website with unlimited access.

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 making 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), click Edit, highlight all of your customizations, and delete them. Click the Save button in this same column and then the Commit button to apply all changes.

The huge 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.

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. 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. Firefox basically 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 into another Twitter account within the same browser. If I open a new tab and go to twitter.com, I am automatically logged into 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.

Finally, I hesitantly recommend **LocalCDN** ([addons.mozilla.org/firefox/addon/localcdn-fork-of-decentraleyes/.org](https://addons.mozilla.org/firefox/addon/localcdn-fork-of-decentraleyes/)), which complements uBlock Origin. Websites have increasingly begun to rely on large third parties for content delivery, such as tracking software supplied by Google, Microsoft and various content delivery networks. Blocking this code which tracks your activity can often break the website you are visiting. LocalCDN provides local files to replace the otherwise necessary content to improve online privacy. As an example, the site riverfronttimes.com requires some code called JQuery. This site loads JQuery from Google's servers, and Google collects usage data about my activity on this site. If I block the request to download JQuery from Google, the site will not load properly. The JQuery code is simply required for this site (and many others) to function. With LocalCDN installed, it intercepts the request to download JQuery from Google and provides a locally stored option instead. The JQuery code is loaded from the browser extension without the need to involve Google. The site loads properly, and Google does not track me. LocalCDN is known to break many sites. If you find a site which displays no text, it may be using resources such as Google Fonts which prohibit third-party interception. Be sure you know how to disable LocalCDN whenever you must access a blocked site. Many readers will become frustrated and simply remove this add-on, which I respect. I often question the benefits versus annoyances.

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 browser, including Brave.

Regardless of your chosen web browser, you should test your configuration for any potential leaks. I rely heavily on the free service **Browser Leaks** at <https://browserleaks.com>. There are numerous options within this site, and I outline my favorite below.

- <https://browserleaks.com/webrtc>: This page displays whether your browser is blocking WebRTC IP leaks as previously mentioned. The goal is to receive all red “False” responses.
- <https://browserleaks.com/geo>: This page identifies whether your browser is sharing location data or the about:config changes we made are blocking it. The optimal response is a red “Denied” result.
- <https://browserleaks.com/proxy>: This page discloses any unique filtering within your network which could make you a more unique visitor to a site. The goal is to receive all red “not detected” results, unless you approve of the technology filter. You may see uBlock filters, which eliminate specific data from entering your session.
- <https://browserleaks.com/social>: This page displays any social networks or online marketplaces which place a login cookie on your machine. As an example, if you are logged in to an Amazon account, you should see evidence of that here. This is a good test to ensure your Firefox containers are functioning properly.
- <https://browserleaks.com/javascript>: This page displays the information available about your connection to any site you visit. Interesting areas include local time, browser identifiers, and operating system data.
- <https://browserleaks.com/flash>: This page displays whether the Flash plugin is installed. My preference is that it is never used.
- <https://browserleaks.com/silverlight>: This page displays whether the Silverlight plugin is installed. My preference is that it is never used.
- <https://browserleaks.com/java>: This page displays whether the Java plugin is installed. My preference is that it is never used.
- <https://browserleaks.com/donottrack>: This page displays your “Do Not Track” browser settings. A display of “1” confirms that your browser is blocking requests to track the user. In Firefox, this can be enabled under the “Privacy & Security” menu, but this option may be redundant with their latest site isolation technologies.

Again, this is not a comprehensive list of digital security best practices for various operating systems. This is the bare minimum recommendations in order to continue your journey through extreme privacy strategies. My scope here is to disappear completely and possess better privacy. My own education on digital privacy and security is never-ending. I learn a new or better way to execute my own strategies monthly.

DNS Configuration

In the simplest explanation, DNS translates domain names, such as inteltechniques.com, into IP addresses in order to locate the appropriate content. In a typical home setup, your internet service provider (ISP) conducts your DNS queries. In other words, your ISP knows every website you visit, regardless of SSL encryption, and knows your billing address. If you did not purchase internet service anonymously, then they also know YOU. ISPs collect a lot of valuable information about you this way, and often sell these details to third parties for marketing purposes. I want to stop that. Whether you use no VPN whatsoever (poor), rely on an application-based VPN directly on a computer (better), or execute a full home firewall as explained later (best), you should modify your DNS settings. First, let's identify the techniques to locate the DNS settings within the three major operating systems.

- **Linux:** Launch “Settings”; click “Network”; open connection configuration; access DNS settings for IPv4 and IPv6; Disable “Automatic”; and add desired servers.
- **Apple:** Launch “System Preferences”; click “Network”; select connection; click “Advanced”; click “DNS”; remove any entries and add your desired servers.
- **Windows:** Launch “Settings”; click “Network & Internet”; click “Change Adapter Options”; right-click connection; choose “Properties”; click “Internet Protocol Version 4”; click “Properties”; enter your desired DNS servers; click “OK”; and repeat for “Internet Protocol Version 6”.

As discussed later in the Home Firewall chapter, I recommend Cloudflare DNS service due to their speed, stability, encrypted options, no-logging policy, wide adoption, and third-party auditing through KPMG. Some may disagree with this choice, which I respect. I believe it is our best option in order to maintain “normal” appearances while taking advantage of the protection. Many prefer niche privacy-focused community-driven DNS providers, but I believe these can make our connections stick out more than widely-used secure options. I also trust the third-party audit of Cloudflare more than unproven promises of smaller operations. You can add server addresses of 1.1.1.1 and 1.0.0.1 to your computers using the previous instructions in order to route all DNS requests through Cloudflare.

There are a few caveats here. If you are using a VPN application on the computer, it will likely ignore your DNS choices and use its own server. This is acceptable for most. If your VPN crashes, you would fall back to Cloudflare for DNS, which provides better protection than being exposed to your ISP. If you are connected to a home firewall, this is redundant, but not harmful. This prevents SOME snooping from your ISP. We should now ensure that our connections are encrypted. Navigate to <https://www.cloudflare.com/ssl/encrypted-sni/> and conduct a test. You should see green checkmarks next to the first three tests. If you do, you are hiding much of your internet traffic from your ISP and your VPN. Firefox is currently working on support for the final security option.

VPN Configuration (Desktop)

I mentioned the importance of a VPN in the previous chapter in regard to your mobile device. This also applies to any computer you use. The same service you selected for your phone should provide an app for your computer. Most reliable VPN providers grant you multiple consecutive device usage. Therefore, you can use the same account credentials on your laptop which you use on your mobile devices. Even if you choose to replicate the home firewall with constant VPN, as explained later, you should still possess a VPN application on your laptop for travel usage. When traveling, I rely on a VPN application any time I am connected to the internet. This is especially important if using any type of public Wi-Fi.

Similar to the previous chapter, I rely on **ProtonVPN** (inteltechniques.com/proton) as my provider for my laptop(s). Installation on a Windows or Mac machine is straight-forward, but Linux will take a few tweaks. Mac users with Brew installed can simply enter “brew install protonvpn” into Terminal. While many popular VPN applications offer a native graphical VPN application for Linux, ProtonVPN currently does not. This is disappointing to many clients, and may change by the time you read this. Instead, ProtonVPN relies on a series of Terminal commands in order to install and configure their “beta” VPN software. Some may see this as a hinderance while others appreciate the dedication to ultimate security which this affords. Either way, it is not too difficult and only required once. If ProtonVPN still requires you to manually configure their Linux client, the following steps apply.

Post-Publication Note: The following steps have changed after ProtonVPN issued a new native Linux application. Updated commands are available at inteltechniques.com/EP.

- sudo apt upgrade
- sudo add-apt-repository 'deb <https://repo.protonvpn.com/debian> unstable main'
- sudo apt update
- sudo apt install protonvpn -y
- protonvpn-cli login (enter your ProtonVPN username)
• (Enter your ProtonVPN password when prompted)
- protonvpn-cli connect
• (Select your desired country, region, and mode [UDP] when prompted)
- protonvpn-cli status

That final command should confirm that you are successfully connected to your VPN. You can also confirm this within the Ubuntu power menu in the upper-right of your system. Next, let's configure the kill switch with the following command.

- protonvpn-cli ks --always-on

Reboot your machine and let's confirm things from a fresh place. If you launch your browser and try to connect to a website, it should be refused. This is because your VPN is not connected and we activated the kill switch which prevents any internet access unless the VPN is running. This is a huge advantage for this method. If your VPN connection fails or you forget to launch it, no data is sent out through an unprotected internet connection. In order to launch the VPN, you could repeat the previous option which allowed you to choose a server. However, I prefer the following option which simply connects to the closest and most reliable server. You can launch this in Terminal upon boot to activate your VPN.

- `protonvpn-cli c -f`

There are scenarios where you may want to disable the kill switch option. If you use your laptop at home while protected behind a network firewall with VPN, as explained in the next chapter, running a desktop VPN application is not recommended. However, if you turn off the desktop VPN, your kill switch prevents any internet access. In these scenarios, the following command disables the kill switch until you re-enable it. Note that you must restart the VPN connection for this to take effect.

- `protonvpn-cli ks --off`

If you use a VPN from your laptop occasionally, I would avoid the steps for the kill switch. If you do not have a router with an embedded VPN, as explained in the next chapter, then I would active that “always-on” kill switch. Understand that your VPN does not automatically launch upon boot. You must activate it within Terminal with “`protonvpn-cli c -f`”. If this seems like a cumbersome daily process, you can replicate my shortcut method with the following commands within Terminal.

- `wget https://inteltechniques.com/EP/VPN.desktop`
- `chmod +x VPN.desktop`
- `sudo mv VPN.desktop /usr/share/applications/`

You should now see a new program titled ProtonVPN within the Applications menu. Clicking this shortcut launches the command to connect to the closest ProtonVPN server. If desired, you could right-click this new icon and add it to your Dock for easy access. If you launch this application while ProtonVPN is already running, it disconnects and seeks the best server again. This is extremely convenient when you notice a slow connection. This shortcut does NOT include a kill switch, but you could edit the “Exec” line in the file to display “`Exec=protonvpn-cli c -f ks --always-on`” to enable this feature. Many will say the process of installing and configuring ProtonVPN for Linux is antiquated. I understand the judgement, but I prefer the manual approach which works flawlessly at all times. I do not need a pretty program with bells and whistles. I prefer something reliable which always works.

Relying on a VPN company is difficult. We place a lot of trust into the provider(s) we choose, without knowing much about the company or their financial backing. I had recommended PIA for many years. Their merger with Kape Technologies has urged me to step away from this endorsement. Kape, previously known as Crossrider, has been heavily focused on advertising and data collection in the past. Access to millions of privacy-minded VPN users' computers could be a goldmine to them. Therefore, I no longer install the PIA application on my devices.

I believe all VPNs are flawed, but still a requirement for us. Almost every VPN provider relies on rented servers across the globe which are out of their control. Many providers unknowingly use the same servers as their competition. A VPN is simply a single layer of protection. Always purchase your subscription anonymously, and I present multiple options for this later. When using a VPN, you are simply placing your internet history into someone else's hands. This sounds bad on the surface, but it is better than doing nothing at all. Without a VPN, we know our ISPs are monitoring, collecting, and sharing our internet activity. With a VPN, we are told that this information is not logged or shared. Are we bullet-proof? No. However, I would rather make the attempt to hide my traffic than do nothing at all.

Some may question the amount of data shared about your online history when you send all of your traffic through a VPN versus your ISP. There are always vulnerabilities which could expose more data than intended, but we can discuss a few misconceptions about your internet traffic. First, we should tackle SSL/TLS. SSL (Secure Sockets Layer) and its successor, TLS (Transport Layer Security), are protocols for establishing authenticated and encrypted links between networked computers. This is related to the lock icon you see in your browser when on any website which begins with "https". This indicates a secure connection, but what does that really mean? I will simplify this technology with a couple of examples.

Assume you are on your home computer connected directly to your internet service provider (ISP). You are not using a VPN. You connect to Google and conduct a search for "inteltechniques". The response URL presented to you, including the search results from the query, is <https://www.google.com/search?q=inteltechniques>. Does your 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. Now, let's introduce a VPN. After connecting to your VPN, such as ProtonVPN, you conduct the same search. 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. Why does this matter?

Everyone has a unique threat model, but I will present a few scenarios where you may be concerned. First, consider that I am suing you civilly, 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 is 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. If you had a VPN enabled, I could only prove your device(s) were connected through a VPN. I would not know any domains from your activity. A second court order to the VPN provider would not reveal this data. Reputable VPNs do not log this traffic, and IP addresses are shared between thousands of users.

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). If the IP address belongs to your VPN provider, it will not disclose any details about you or the VPN account. A subpoena to the VPN for information about the IP address will reveal no logs and an education about IP address sharing between thousands of strangers.

Now, let's combine the strategies mentioned previously to thwart this behavior. Since you are always connected to a VPN, your ISP knows nothing about your internet traffic. A subpoena to them would not reveal the sites you visit. Since ProtonMail does not log your IP addresses in clear text, they cannot determine your true IP address. Since ProtonVPN and ProtonMail are Swiss-based companies, they would not respond to a subpoena from the U.S. If you purchased a VPN service without providing your name, there is nothing to glean from the VPN provider about your account (such as a personal credit card number or home address). I hope that you now see that all of these strategies strengthen each other.

What do I do? At home, my entire network is behind a fail-proof VPN. I will explain each detail in the next chapter. I do not need individual VPN applications running on my devices while at home. While traveling, I have the ProtonVPN desktop application ready on my laptops. As mentioned previously, I have the ProtonVPN app installed on my mobile device. Many readers may be tired of my promotion of ProtonVPN. After all, it requires a valid email address and some type of digital payment (Bitcoin is accepted). If you want a solution for privacy which accepts cash, consider **Mullvad** (mullvad.net). On their website, you generate an account without providing any personal details. A unique account number is issued to you. Once you make payment for that account number via Bitcoin or mailed cash, the account is enabled. This is likely overkill for most people, but a truly anonymous solution is nice. Current annual pricing for ProtonVPN is \$48 and Mullvad is \$65. However, your VPN choice should never be based on price alone.

Email Usage

I believe I could devote an entire chapter to numerous options related to email usage. In the previous edition, I provided multiple email strategies which was overwhelming to many readers. In this edition, I will only present the exact methods in use by my clients and myself. This provides explicit detail which can be replicated without the need to determine the best route for your own situation. There are many ways to create a secure email strategy, and I do not claim mine to be the best. It is simply the most appropriate option for me and my clients. The following summarizes each step of my email strategy, which is outlined in detail within the following pages.

Encrypted Email Provider (ProtonMail): First, we establish a private and secure email provider. ProtonMail checks all of the boxes for my usage, as explained soon.

Alias Email Addresses: Next, we configure the five accounts provided with any paid tier of ProtonMail. This allows us to send and receive email from five different accounts, displaying five different names to the recipient, without the need to log in to multiple accounts.

Email Forwarding from Previous Provider: After we configure our new email account, we need to receive email being sent to our previous accounts without accessing those services. We will forward email to our new ProtonMail account.

Masked Email Forwarding: Next, we will establish a masked email forwarding service which will protect the identity of our true accounts within ProtonMail. This provides numerous options to give to “junk” services which demand an email address.

Custom Domain Email Addresses: This is the strongest piece of our strategy. We will purchase a custom domain and associate it with our ProtonMail account. This provides unlimited addresses without relying on the protonmail.com domain.

Offline Email Archive: After we have everything configured, we should occasionally retrieve all email messages into an offline archive for use in the event of internet outages, catastrophe, or service disruptions.

Email Privacy Concerns: Finally, we acknowledge various email privacy concerns and modify our behavior to avoid any traps.

Encrypted Email Alternatives: If ProtonMail is not appropriate for your needs, I present alternatives which possess the same privacy and security benefits.

Let's get started.

Encrypted Email Provider (**ProtonMail**)

All of my clients are given a new primary email address through the service **ProtonMail** (inteltechniques.com/proton). This service with a free tier provides Switzerland-hosted communications with true zero-knowledge data. 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 ProtonMail would be unable to view any message content. If an email is sent from one ProtonMail 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 ProtonMail, 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 that may not be accepted by the security community. First, email is broken. It is outdated and was never meant to be private. I assume every email I write could be seen by someone else. I trust services such as ProtonMail 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.

Some will wonder why I don't use Tutanota or other zero-knowledge providers. It is mostly due to adoption. Most people in my circles have ProtonMail and no other secure options. The more messages I can keep within one single encrypted ecosystem the better. However, I will identify options later for those with unique situations.

The primary ProtonMail email address created when opening a new account should be used only for communications associated with your real name. This could include your family, colleagues, or anyone else who knows your true identity. I recommend including your true name within this address, such as john.smith@protonmail.com. This is your new primary email account. It should possess a very strong password and two-factor authentication. I prefer Authy for this, as explained previously. Once you have an account, we can explore the benefits of paid accounts. You can order a free or paid account with the latest discounts on my site at inteltechniques.com/proton.

Alias Email Addresses (ProtonMail)

While a free ProtonMail account is fine for minimal usage, we will need a paid account to complete our email strategy. The “Plus” tier is suitable for most users. If you exceed a specific resource provided within this tier, you can increase individual thresholds as needed. Paid accounts include alias email addresses which can be accessed within the main account. I find the simplicity of one inbox and ability to send emails from multiple addresses within a single web client or mobile application to be extremely beneficial. There is no need to overly complicate things, and convenient options will be used more consistently than difficult tasks. The following is a typical scenario for the five email aliases provided by ProtonMail.

- **real.name@protonmail.com:** This account is considered a public email address, and is provided to family, colleagues, or anyone else who knows your true identity. It is an address that will be publicly visible eventually. Data mining companies and credit bureaus could eventually identify this as your primary email account.
- **alias.name@protonmail.com:** This account is in the name of an alias. This allows sending and receiving mail in a unique generic name. This can be vital when a home is titled in an alias name and the client wants to have immediate access to email messages intended for that recipient. It allows you to hide your true identity, but enjoy the benefits of secure email without multiple login requirements.
- **purchases1980@protonmail.com:** This account is used for all online purchases. The generic name allows usage with any alias or real name. This will likely be shared with third-party affiliate services and data mining companies. This could also be associated with travel-related purchases. I assign the name “Purchasing Department” to this alias address, which is visible to recipients.
- **number@protonmail.com:** This is a generic account with no personal identifiers, similar to 1980@protonmail.com. It can be used for practically any purpose without disclosing any name. It is often used for items which are not vital, but need to be received, such as a receipt from an in-store digital purchase. I assign the name of the number, such as “1980”, to this alias address, which is visible to recipients.
- **catchall@customdomain.com:** We will associate a custom domain name to your ProtonMail account which will be configured as a “catchall” address. This will allow you to receive email from unlimited addresses and send from a generic account. A “Professional” tier account is required for this feature, as explained later.

When you create your ProtonMail account, you will provide a name for association with any addresses. When you send an email, this name is visible to the recipient. It is vital to configure the desired name for each address before usage. While logged in to your ProtonMail account, click on “Settings”, “My Addresses”, then “Edit” next to each address. You can then change the name attached to each. There are many additional options for your five addresses. Use the previous summary as a starting point to determine your best strategy.

The next step I recommend is to create folders for every address. This will make it easier to identify which email is associated with a specific account. Conduct the following.

- Navigate to “Settings” > “Folders/Labels” > “Add Folder”.
- Create a new folder for each email account.
- Navigate to “Settings” > “Filters” > “Add Filter”.
- Create a new filter for each email address.

The following is an example which will route all of my incoming mail to the address of purchases1980@protonmail.com to the folder I created titled Purchases.

Name: Purchases

Conditions: If the recipient is exactly purchases1980@protonmail.com

Actions: Move to Purchases

Repeat this for each email alias. When finished, you should have all alias accounts listed in the lower left corner of your email portal. You can now easily identify which alias account received a message, and will be less likely to respond as your real name. No messages will appear in your global inbox, which provides isolation. Each folder will display an indication that a new message has been received.

While ProtonMail possesses great privacy and security with the default settings, there are things which can be improved. I apply the following for all clients.

Disable remote images: Many email images contain tracking pixels which identify the IP address and device information when opened. Click on “Settings”, “Account”, then change “Load Embedded Images” to “Manual”. Next, change “Request Link Confirmation” to “Enabled”. This will prompt you for authorization to open any links within a message. This prevents accidental link clicking, and displays the entire URL before opening.

Disable Auto-Contact Storage: By default, ProtonMail saves the contact details of any outgoing messages, including responses. This leads to a contact list full of people who are rarely contacted and leaves potential evidence of sensitive associations. I prefer to disable this option completely at “Settings” > “Account” > “Automatically Save Contacts” > “Disabled”.

Account Access: Most ProtonMail users access their account from the official website at protonmail.com. I always prefer to use the Beta site at beta.protonmail.com. This always presents the latest features which are being tested, but have not been released publicly. I bookmark this page to make sure I access it instead of the main page. I use the ProtonMail app on all mobile devices, including my primary GrapheneOS unit. For that purpose, it can be installed via the Aurora Store, as previously explained.

Email Forwarding from Previous Provider

You likely have a current personal email address that you have been using for several years. This may be a Gmail, Yahoo, Hotmail, or other free provider. I recommend ceasing all outgoing activity from these accounts. These companies have the ability to monitor your communications and will provide all of your content if presented a court order, even as a result of a malicious civil lawsuit. An employee with ill intent has the ability to export all communications and send them to anyone willing to pay the appropriate fee for this illegal service. We simply cannot trust any company to access our most sensitive messages.

However, I never recommend deleting any accounts. If you start using your new ProtonMail account for all of your personal communication, that does not eliminate the need for your old accounts. You will continue to receive desired email through these accounts, and you may need to use an old account to verify your identity to a service such as your bank. Instead of manually checking these accounts, consider forwarding all of your email to your new ProtonMail account after you archive and delete all stored content (as explained momentarily).

All major email providers allow you to forward incoming email messages to another address. This allows you to receive the emails being sent to your old accounts without logging in to the services (and providing details about your computer and connection). You will not be able to send email from these old accounts, but that should be avoided anyway. All of your email to old accounts will appear in your new ProtonMail account. Any outgoing message will be from this ProtonMail account. The following steps will forward your email from the old accounts. If yours is not listed, an internet search will provide all you need.

- Gmail: “Settings” > “Forwarding and POP/IMAP” > “Add a Forwarding Address”
- Yahoo: “Settings” > “Accounts” > “Forward”
- Microsoft: “Settings” > “Options” > “Mail” > “Forwarding” > “Start Forwarding”
- Apple: “Preferences” > “Forward my email to”
- Fastmail: “Settings” > “Filters & Rules” > “Create New Rule”

Overall, think of your new ProtonMail address as your primary email account, replacing anything previously used, such as a Gmail account. It should only be used for desired communications. It is your personal email account and can be registered in your real name. I actually recommend this in case you ever need to prove yourself as the true owner. Know that your stored email messages cannot be accessed by anyone without your authorization, including ProtonMail employees, criminal hackers, or governments. Try to avoid using this address for newsletters and junk registrations. You should consider creating a masked forwarding account for anything that is not vital to you, as explained next.

Masked Email Forwarding

For the past several years, all of my clients have received a free email forwarding account from **Blur** (dnt.abine.com), **AnonAddy** (anonaddy.com), **33Mail** (33mail.com), or **SimpleLogin** (simplelogin.io/?slref=osint). Some clients activated accounts at all four services. Today, I only configure an account with SimpleLogin in order to simplify the benefits of email forwarding services. These companies protect 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 (ProtonMail) email account. These prevent 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.

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. Let's begin with a typical configuration for a client.

I create a free account, providing the alias ProtonMail email address during registration. I believe that all forwarding email from services such as SimpleLogin should be sent to the alias account instead of the primary address. This prevents SimpleLogin from knowing your true identity. I then activate two-factor authentication (2FA) within the "Settings" link. I use Authy for this security. 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 may be used when websites demand an email address in order to remove my personal information from their websites, which is explained later. 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 alias ProtonMail 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 ProtonMail 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 Blur, AnonAddy, SimpleLogin, or 33Mail 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.

If forced to provide my next recommendation, it would be AnonAddy. I no longer use Blur or 33Mail due to global recognition that these are forwarding services. Many sites refuse their addresses due to abuse. To be fair, this could happen to SimpleLogin eventually.

Let’s pause and take a look at this strategy of email usage. Assume your alias ProtonMail address is joe.johnson@protonmail.com. 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. This allows me to generate a unique address for every need. This also provides an option to assign my own custom domain with their service, but I do not do this. I will explain my preference for a custom email domain next.

Custom Domain Email Addresses

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 the previous examples. In each of those, 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 should lose your access to that account? In those scenarios, I chose ProtonMail as my email provider and SimpleLogin as my email forwarder. What if they disappeared, terminated my account, or suspended my access due to suspicion of fraud? While all of this is extremely unlikely, the chance still exists. Therefore, I prefer to take advantage of the secure hosting provided by ProtonMail while controlling the avenues of communication with my own domain. This will require many steps, but the end result is worth the effort.

A “Professional” tier ProtonMail plan is required in order to bring in your own domain with catch-all support. I prefer to pay via Bitcoin, but an “anonymous” debit card could also be used (both are explained later). A paid domain registrar is also required in order to secure a custom domain name. For domain registration, I prefer Namecheap. However, I never recommend their other products. I find their web hosting to be awful compared to other providers, but their domain services are ideal. Namecheap provides affordable domains and includes their own WhoIs privacy service for free. This masks your registration information from public view. Some registrars charge up to \$20 annually for hiding these details. Our first step is to secure a domain name. What should you choose? Here are three considerations.

- **Don’t Choose Your Name:** You may be tempted to secure your real name within the domain, similar to michaelbazzell.com, but this has many disadvantages. While it works well when giving out an email address while using your true identity, it appears suspicious when trying to use an alias. Bob.Smith@michaelbazzell.com would raise some eyebrows and give away your real name.
- **Keep It Generic:** 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” from Namecheap for \$2.88 with a \$6.88 annual renewal. 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, create an alias email account such as bob.smith@securemail.work, or become generic such as office@securemail.work. I also created a landing page at 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, I rely on michaelbazzell.com for most work email addresses, including accounts configured for employees, which are all hosted at ProtonMail.

During checkout, Namecheap will demand to know your real name and physical address. While they do not share this publicly, they can sell and share it with third-party partners. Using John Doe at 1212 Main Street will earn you a quick account suspension from Namecheap, as false information violates the rules imposed by the Internet Corporation for Assigned Names and Numbers (ICANN). Their policies require you to be honest about the details you provide. This puts us in quite a predicament, but I have a solution that may work well for some.

During my purchase, I created a new Namecheap account, provided my first name as “M”, my last as “Bazzell”, and placed my order with a Privacy.com card (explained later). During checkout, Namecheap demanded a full name, physical address, telephone number, and email address of the registrant for the domain. While you could lie on each of these, you risk losing the domain and you would be violating ICANN rules. Instead, I again provided “M. Bazzell” as my name, and the full mailing address of the hotel where I was staying at the time. I even included the room number in order to be transparent. Technically, this was my current physical residence.

I supplied my “Purchases” ProtonMail email address and a VOIP telephone number which I could access if needed. I executed the purchase, and my new domain was generated. My total cost was \$3.06. I provided my true name, my true current physical address, an email address which forwarded to my ProtonMail inbox, and a VOIP number which forwarded messages to my email. I believe all of these details were accurate at that moment in time, and I violated no ICANN rules. You may disagree.

Next, I needed to configure this new domain to forward messages to my ProtonMail account, and configure my ProtonMail account to receive the messages sent to that domain. The following steps walk through the process at the time of writing.

- In the Namecheap dashboard, I clicked the “manage” button next to my new domain.
- In ProtonMail, I clicked “Settings”, “Domains”, then “Add Custom Domain”.
- In the ProtonMail pop-up menu, I entered securemail.work as my domain.
- In the Namecheap Domain settings, I clicked “advanced DNS”.
- I then clicked “Add New Record” in the “Host Records” menu.
- As instructed by ProtonMail, I chose “TXT Record”, “@”, and the values presented in the ProtonMail configuration pop-up within the Namecheap settings.
- In the ProtonMail dialogue, I clicked “Next”.
- In the “Add Addresses” dialogue, I entered EP@securemail.work and a name of Secure Mail. I clicked “next” and allowed ProtonMail to generate my new keys.

- I clicked the “MX” button in the ProtonMail configuration menu.
- In Namecheap, I chose “Custom MX” in the Mail Setting menu. I then provided the custom settings displayed in the ProtonMail dialogue, visible in Figure 3.03.
- I added the SPF record into Namecheap as instructed by the ProtonMail dialogue.
- I added the DKIM record into Namecheap as instructed by the ProtonMail dialogue.
- I ignored the DMARC options and closed the ProtonMail pop-up window.
- When finished, I checked the “Catch All” option next to my new email address.

Within an hour, the settings were applied and ProtonMail was happy with my configuration. Figure 3.04 displays my TXT records applied with the previous instructions.

Type	Host	Value	TTL	
MX Record	_@	mail.protonmail.ch	10	Automatic
MX Record	@	mailsec.protonmail.ch	20	Automatic

Figure 3.03: MX records for a custom domain.

Type	Host	Value	TTL	
TXT Record	_@	protonmail-verification=███████████	Automatic	
TXT Record	@	v=spf1 include:_spf.protonmail.ch mx ~all	Automatic	
TXT Record	protonmail._domain	v=DKIM.kvval.pvt ██████████	Automatic	

Figure 3.04: TXT records for a custom domain.

Let’s pause and reflect on what we have accomplished. I purchased a domain name of `securemail.work` semi-anonymously. The details of this registration are hidden from the public. I created a paid ProtonMail account. I forwarded the mail servers of the domain name to the ProtonMail service. I configured both a real email address and a wildcard address within ProtonMail. Any email sent to my domain is received in my ProtonMail account. If you send an email to `EP@securemail.work`, `12@securemail.work`, or `ihatethisbook@securemail.work`, it will get to me. I can provide an unlimited number of email addresses for this domain, and all will end up in my inbox.

This 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 ProtonMail can view my messages. If ProtonMail should ever become unavailable, I can forward my domain within Namecheap to a new email

provider and continue to access my accounts. As of this writing, over 90% of my communications are conducted within my own domain associated with my ProtonMail account. I believe this is the best email strategy.

If Namecheap refuses to activate an account due to fraud, or demands a “selfie” to prove your identity, I recommend replicating these steps with the service at **Hosting Matters** (hostmatters.com). If you encounter any issues there, tell them you are reading my book. They should unlock your account, as they have a deep respect for privacy.

Always create an account with a domain registration service BEFORE purchasing a domain. Make sure the provider does not flag your account as suspicious before locking in a desired domain with that service. Never rely on this new domain until you are confident that the registration provider has not flagged your account for review. Unfortunately, this is always a concern when we refuse to provide our true home address and cellular number to an online service provider.

You may be questioning my inclusion of a real last name with my domain registration. I do this for the following three reasons.

First, I do not want to risk losing the domain. If ICANN or the domain registration provider should demand proof of my identity in order to keep the domain, I want to be able to do so. I can't risk someone else buying my domain because I cannot prove I am “John Doe”. It could allow someone to buy my domain and impersonate me with real email addresses.

Next, Namecheap protects my details from being publicly released with their free WhoIs privacy service. This is not perfect and there is always a chance of exposure, but it is minimal. My provided physical address and contact details are not personal, so there is not much threat.

Finally, this domain will often be used in my real name. It is likely that an email address such as michaelbazzell@securemail.work will leak out eventually, so the association to my name will be obvious anyway.

My final thought on domain registration is that there is a balance between privacy and security. If I claim to be John Doe, I risk losing the domain. If I provide all accurate details, I risk exposure. I find the previous strategy's balance to be appropriate. I prefer to provide my real name when purchasing any domains which will be publicly associated with my true identity. I will be able to prove my identity if something bad should happen. If I need something completely private, such as a website displaying controversial content, I will purchase the domain anonymously with Bitcoin at **Njalla** (njal.la). However, I would never use a domain from this service for email. Njalla technically owns the domain and you just pay them to use it. There is a higher risk of domain loss with a service such as this.

Business Email Considerations

All of the email options I have presented assume you need access as an individual. This is the most common scenario I have experienced with my clients. However, you may have more advanced needs. If you own a small business, you may want multiple employees to access their own email accounts within the same custom domain. You may currently have email addresses assigned within your domain registration and hosting service and employees may log in there via a web portal. If so, all messages are exposed in the same way which Gmail and other non-encrypted providers could be abused. I offer two options for these situations.

ProtonMail: Professional and Visionary paid tiers offer support for additional users. You can assign specific email addresses within your custom domain to unique user accounts. These accounts can be accessed by other people. You maintain all of the benefits of E2EE as you would with an individual account. You can also add extra storage as needed.

My complaints about this method are two-fold. First, each account is allowed only 5GB of initial storage. If starting a new account, this should be sufficient for a while, but importing any email messages will quickly deplete this allotment. Next, the pricing is steep for the space. At \$75 annually per user, five employees and yourself will cost \$450 annually. You might consider the Visionary plan which allows six users to share 20GB of storage for \$288 annually. It also offers more custom domains and addresses. Finally, the Visionary plan provides unlimited access to ProtonVPN. Always consider these package deals.

Fastmail: This service does not provide E2EE communications. It is a traditional email service and all communications are accessible by the provider. I present it here as an appropriate option within some business scenarios. Fastmail is the best traditional email provider I have found. My training company uses it for all email sent to our custom domain. I can assign unique addresses to each user or configure single addresses to forward to multiple people. The cost is \$50 per user annually which allows up to 30GB of storage for each employee. That is very robust for the cost. This includes access to shared calendars, notes, and contacts. Again, none of the data is completely encrypted. I believe this is a great option for small businesses considering that the majority of your messages will be associated with other addresses which are also not E2EE.

Fastmail is an Australian company. They monetize all of their services and provide no free tiers. Their business model is simply fast and efficient email. A court order from an Australian government will indeed disclose any targeted communications. I use Fastmail for two of my domains which include email addresses which need to be monitored by multiple employees. My privacy consultation domain (michaelbazzell.com) is hosted on ProtonMail with addresses accessed by two employees. Either of these methods can work in these scenarios, and you should consider the overall sensitivity of your communications before making any decisions.

Offline Email Archive

The ProtonMail paid plans include unlimited usage of the Import-Export utility available on their website at <https://protonmail.com/blog/import-export-beta>. This tool easily exports all of your messages for archival purposes. More importantly, it allows you to import all of your content from your previous email provider. If you had a Gmail account for several years, you likely possess messages which need to be accessed on occasion. You can import all of this content into your ProtonMail account for easy access without logging in to your previous account(s). Be sure to pay close attention to the storage requirements. I prefer a different strategy for most clients.

Whether you use a Mac, Windows, or Linux machine, I highly recommend possessing a backup of all email, calendars, and contacts. I rely on an open-source third-party solution called **Thunderbird** (thunderbird.net). This product is a very minimal open-source email, contacts, and calendar application. I do not recommend using it for daily access to these services, 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? Do you know all of your upcoming appointments without relying on your online calendar? 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 Thunderbird allow you to specify the settings of your accounts, and then keep your entire email, contacts, and calendars 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. Calendars sync via CalDAV and contacts sync via CardDAV. However, we will not use these protocols.

Encrypted email providers, such as ProtonMail, present a difficult scenario. Since the email is fully encrypted, they do not allow standard IMAP access from a third-party client. However, ProtonMail addresses this with their bridge and export applications. Available only to paid accounts, these utilities allow an email client to download all messages from their servers. This provides a full backup, the possibility of offline access, and full search capabilities within the content of the messages. Installation of the bridge application through Windows or Mac is very straight-forward. The Linux installation can be awkward. Let's set it up together.

- Within Linux, navigate to <https://protonmail.com/bridge/install>.
- Download the “.deb” file under the Linux option.
- Open the Files application and right-click the downloaded file.
- Select “Open with Software Install” and click “Install”.
- From the Applications menu, launch the ProtonMail Bridge program.
- Click “Okay”, “Add Account”, enter your credentials and 2FA, then click “Next”.
- Quit the Bridge app, reboot, and confirm account is present upon launch of Bridge.

Now that you have the bridge application installed and configured, you have a direct connection from your Linux operating system to the ProtonMail environment. Regardless of your operating system, we must now configure the email client. The following steps should apply to Linux, Windows, or Mac computers.

- Launch Thunderbird, which should present an email configuration menu.
- Enter your name as configured with your primary ProtonMail address.
- In ProtonMail Bridge, under “Accounts”, expand the username account menu.
- Click “Mailbox configuration” and copy the username.
- Paste the username into the Thunderbird email configuration menu.
- In ProtonMail Bridge, copy the generated password.
- Paste the password into the Thunderbird email configuration menu.
- Click “Continue” and “Done”.

If you receive an error about your account, you may need to verify your account is present within the Bridge app and reboot. I had to repeat these steps. You will receive an error about a security certificate once the connection is made. This is expected behavior. You can safely click “Confirm Security Exception” when this happens. Thunderbird should begin collecting your ProtonMail email, which could take a long time.

I only use this only as an offline backup of all email in the event I cannot access my ProtonMail 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 Thunderbird 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. I explain this process with your encrypted contacts in just a moment. Some readers may be aware of a free program called ElectronMail which allows ProtonMail users to retrieve their offline messages through a native application. This is a well-respected option, but it is not an official ProtonMail project. While it is open-source software, I would never allow any third party to intervene within my secure encrypted email. Therefore, I do not recommend this application for those seeking extreme privacy.

Our next concern is your “old” email account. 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 ProtonMail. I wanted all of those messages in both my offline archive and my online ProtonMail 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 ways to archive and remove the messages, and I will walk through each. You should be able to replicate this overall method with other traditional email providers.

Import & Archive: If using ProtonMail, 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 ProtonMail email address. ProtonMail offers an option to import all email from Gmail, Yahoo, and Outlook through a traditional web browser. Navigate to <https://beta.protonmail.com/u/0/settings/import> while logged in to your account and follow the tutorial. Once all of your email is within your ProtonMail account, you can synchronize to your offline email client, such as Thunderbird, and you will have all email stored securely online and locally. Be sure that your storage within ProtonMail supports the data within Gmail. This may exceed your storage quota.

Archive Only: If you do not want to bring in all of your old email into your new account, you could still archive it all through your mail client. If you know you want to delete the originals from the old email host after retrieval, you can choose the “POP” protocol. This retrieves email from a provider such as Gmail and then removes the original from Gmail’s servers. I typically avoid this strategy because something could go wrong. Instead, I enable “IMAP” within Gmail (“Settings” > “Forwarding and POP/IMAP” > “Enable IMAP”); launch my email client (Thunderbird); configure a new account (“File” > “New” > “Existing Mail Account”); and follow the directions. When complete, you should see all of your old email within Thunderbird as a locally-stored copy. Be sure to move all of these messages into “Local Folders” in order to prevent Gmail from deleting them on a future synchronization. I also prefer to disable synchronization by right-clicking on the new account within the mail client and disabling all options under “Server Settings”, such as “Check for new messages”. If paranoid, you could also change the password here to something inaccurate to prevent accidental synchronization and deletion.

Delete Originals: Regardless of your import or archiving strategy, I believe it is important to delete all email from the old service. Otherwise, all of your previous communication is 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 reversible, so make sure you have all data and a backup in place.

Email Privacy 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 ProtonMail, 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.

A larger concern is exposing your time zone within every email response. While services such as ProtonMail 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. Mac and Windows users can right-click a file to remove metadata, which may be displayed as "Personal Information". If you are using Linux, I prefer a program called Mat2. After installation with the following two commands within Terminal, 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.

- sudo apt update
- sudo apt install mat2 -y

Encrypted Email Alternatives

ProtonMail is not the only encrypted email provider. Tutanota and CTemplar are very respectable choices with free tiers. They provide a similar service to ProtonMail and I believe you could replace ProtonMail with these services in most of the previous tutorials to produce a similar result. I choose ProtonMail due to high adoption within my circles. If you see your contacts mostly using Tutanota or CTemplar, it might be more appropriate for you to use these services. Currently, 75% of my email correspondence from within my ProtonMail account is to other ProtonMail users. Less than 5% is to Tutanota addresses and very few are sent to CTemplar accounts. Therefore, it simply makes most sense for me to stick within the ProtonMail ecosystem. Tutanota and CTemplar both offer a free tier, and I encourage you to create accounts to test their services. The following are some considerations for each.

Tutanota (tutanota.com) delivers end-to-end encrypted email, contacts, and calendar services. They are based in Germany and have a strong history of respect for privacy. However, they are based in a Fourteen Eyes country, which may make a few readers nervous. They provide mobile and desktop applications and have a nice web-based interface. I have found their web interface to work well, but the mobile app is quite slow. They offer shared encrypted calendars, which is quite unique. Two paid accounts can share a single calendar, and each user can modify any entries. I find this valuable for families and work colleagues. There is no option to connect an account to a traditional desktop email client, but their desktop application will eventually store email within the host computer for offline usage.

CTemplar (ctemplar.com) is headquartered Iceland, which is not a 14-eyes country. Their web, mobile, and desktop applications are slick and responsive. The paid tiers seem overpriced to me, but I maintain a free account for use with anyone who relies on this service for secure communication.

ProtonMail, Tutanota, and CTemplar all offer the following:

- E2EE communications within network
- Options to send encrypted messages to emails outside of their network
- Open-source applications and technologies
- No third-party analytics services within login pages or applications
- No third-party metadata collection during usage
- Free tier
- Paid tier business model
- Custom domain email accounts
- Custom domain catchall accounts
- Two-factor authentication

Encrypted Calendar and Contacts

In 2020, ProtonMail began offering an encrypted calendar service. I believe that possessing an 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 don't. Therefore, my calendar is protected through ProtonMail and only visible to me. Currently, there is no option to export a ProtonMail calendar for offline storage. This is unfortunate, and will hopefully be resolved in the future. If it is, exporting an ICS file and importing that file into Thunderbird should provide a reliable backup.

ProtonMail has always supplied encrypted contacts as part of their email packages. These details are also extremely sensitive. I would never want to expose the cellular telephone numbers, home addresses, and employers of my clients, friends, and family. Storing this content within products provided by companies which make profits from data sharing, such as Google, is irresponsible.

Please note that ProtonMail encrypts only the fields after Name and Email. The names and addresses of your contacts cannot be fully encrypted due to overall function requirements. I believe this is acceptable to most low-threat readers. If you have all of your contacts stored within ProtonMail, consider keeping a copy within Thunderbird. The following explains the process.

- Navigate to your ProtonMail contacts at <https://contacts.protonmail.com>.
- Click “Settings” > “Export” > “Export Contacts” > “Save”.
- Launch Thunderbird and click “Address Book”.
- Click “Tools” then “Import”.
- Select “Address Book”, click “Next”, choose “vCard file” and click “Next”.
- Select the VCF file downloaded from ProtonMail Contacts.

I stored all of my contacts within ProtonMail for a few months, but eventually moved on to a more secure option, which is explained next. Using ProtonMail for E2EE email, calendar, and contact details is the most appropriate and convenient option for most readers, and the privacy and security is strong. Most clients go this route, as explained at the end of the chapter, which is completely acceptable. Next, I provide my own preference, which is a bit extreme.

Locally-Stored Contacts

My contacts are extremely important to me. My clients trust me with personal cell numbers, private email addresses, and the locations of their homes which are not otherwise associated with their true names. My contacts are almost as sensitive as my passwords. Because of this, I go to great lengths protecting them. There are many scenarios which I now never allow, such as the following.

- I do not store them within my phone's stock contacts app because it is often prone to abuse by apps and synchronizes content to Apple or Google by default.
- I do not store them within services such as Apple, Google, or Fastmail because they could be abused by a rogue employee or a data breach.
- I no longer store them in ProtonMail because the name and email fields cannot be encrypted, but the phone, address, etc. are encrypted, visible only to me.
- I no longer store contacts within any online platform because I would not have access to the data in the event of an internet outage or contact service disruption.

I no longer want my contacts anywhere online, much like I never store my passwords online. While there are great options, such as ProtonMail, there are still weaknesses which must be monitored. I have decided that all of my contacts will ONLY be stored offline. This presents a dilemma since I need my contacts with me at home (Linux laptop and iPod Touch), and on the road (mobile). This leaves me with two options. I can export my online contacts and import the file into offline contact applications or transfer all contacts to a password manager.

The first step with either method is to export any online contacts as a “VCF” or “vCard” file. Below are examples for three popular email providers. You should find specific instructions for other providers with an internet search.

ProtonMail: contacts.protonmail.com > “Export” > “Export Contacts”

Fastmail: fastmail.com/contacts > “All contacts” menu > “Export” > “vCard 3.0”

Gmail: contacts.google.com > select contact > “Select All” > “More actions” > “Export”

You can delete your contacts within the previous online storage with the following.

ProtonMail: contacts.protonmail.com > select all > “Delete”

Fastmail: fastmail.com/contacts > select all > “More” > “Delete”

Gmail: contacts.google.com > select contact > “Select All” > “More actions” > “Delete”

Now that you have a VCF file of your contacts, you can import them into a traditional contact manager, or wait for my preferred option as explained on the next page.

Linux: When I made the full-time switch to Linux, I assumed there would be plenty of suitable contact management applications. I was wrong. Staples such as Thunderbird only import names and email addresses, and open-source options such as Mailspring require association with an online account through their servers. You could install an email client called Evolution (`sudo apt-get install evolution`) which can import contacts (“File” > “Import” > “Next” > “Import a single file” > “Next” > [select your VCF file] > “Next” > “Next” > “Apply”). You would then have easy access to the data.

GrapheneOS: The stock “Contacts” app allows import of a VCF file (“Settings” > “Import”). If you only need your contacts on that device, this is a very safe and clean way to store data.

macOS: As long as you have disabled iCloud and have not provided an Apple ID, there is likely no harm in using the default Apple Contacts software application. Clicking “File”, “Import”, and then selecting your exported file brings in all of the contacts.

iOS: Since an Apple ID is required for any iPhone system, and iCloud is often enabled by default, I never store contacts within the default iOS application. I have been unable to find a suitable contacts replacement for iOS. Therefore, I typically recommend the KeePassXC strategy or ProtonMail Contacts option, both of which are discussed momentarily.

Windows: I never recommend storing contacts within the native Windows Contacts application. If Windows is your primary host, consider the option within the following pages.

There is a problem here. The contacts within each application have no synchronization option. If you update or add a contact on your laptop, that change is not reflected within your mobile device. Using online sync options such as iCloud have their advantages, but also carry risk. Since I refuse to synchronize and store contacts via the internet, I am forced to use a manual update process. This is why I choose to store my contacts within KeePassXC, as explained within the following pages. Updating contacts is as easy as replacing the database file. I consider the copy on my laptop as the primary database to which I make any changes. The mobile versions are “read-only” and updated on occasion.

I realize we are going a bit far down the privacy rabbit hole. Choose the option best for your needs. I have many clients who do not object to storing their contacts within ProtonMail. They have easy access across web and mobile, and only the names and email address fields are not encrypted. I don’t judge anyone going that route. I apply extra scrutiny toward myself solely due to the contact data being associated with high-risk clients.

KeePassXC Contacts

I have decided to use a password manager for my contacts, which securely stores any sensitive content. I have hundreds of contacts, even after pruning people with which I no longer communicate. Manual entry is out of the question. Since I had everything in ProtonMail, I used their export feature to create a VCF file. A typical partial entry looked like this:

```
BEGIN:VCARD
VERSION:4.0
TEL;PREF=1;TYPE=voice;(202) 555-1212
TEL;PREF=2;TYPE=voice:303-555-1212
ADR;TYPE=x-adr:;;1234 Main;Houston;TX;77089;USA
ORG:Privacy Corp
NOTE:We met at Blackhat
FN:John Doe
item1.EMAIL;TYPE=x-email:doe@protonmail.com
END:VCARD
```

Note that I could have exported the same type of file via Fastmail and Gmail with a protocol of vCard 3.0 or higher. A typical CSV export would have been missing phone numbers if more than one entry for personal numbers was present. I always prefer VCF files over CSV. Now that I have a single file with hundreds of contacts, I need to clean it up. I cannot import this file into my password manager (KeePassXC) unless I have one clean entry per line. I also need a single field with the full name of my contact, followed by all of the remaining data colon delimited. The full name cannot possess a comma because we need everything to import correctly, and KeePassXC sees a comma as a delimiter.

First, I want to rename the downloaded VCF file to “contacts.vcf” and place it on my Desktop. Then, I want to remove the unnecessary lines with the following commands within Terminal on Linux. I focus on Linux since this is an advanced strategy. Either an Ubuntu host or virtual machine, as previously explained, will suffice for this task. All of the commands in this section are available on my website at inteltechniques.com/EP and can be copied and pasted in one action, which is highly recommended over manual entry.

```
sed -i '/^VERSION/d' contacts.vcf
sed -i '/^UID\:/d' contacts.vcf
sed -i '/^PRODID\:/d' contacts.vcf
sed -i '/^item1\.X/d' contacts.vcf
sed -i '/^END\:/d' contacts.vcf
sed -i '/^REV/d' contacts.vcf
```

I now have entries such as the following.

```
TEL;PREF=1;TYPE=voice;(202) 555-1212
TEL;PREF=2;TYPE=voice:303-555-1212
ADR;TYPE=x-adr;;1234 Main;Houston;TX;77089;USA
ORG:Privacy Corp
NOTE:We met at Blackhat
FN:John Doe
EMAIL;TYPE=x-email;jdoe@protonmail.com
```

I need all of the data on one line per contact. The following two commands eliminate all line breaks and then separate each contact, and renames our working copy to contacts.txt.

```
tr -d "\n\r" < contacts.vcf > contacts.txt
sed -i 's/BEGIN\:/VCARD/\n/g' contacts.txt
```

I want all of my telephone numbers to appear as ten digits without hyphens, periods, or parentheses. This is because some dialers need a pure number. The following cleans this up, and I executed each of these a few times.

```
sed -i 's/(\\([0-9]*\\))\\([0-9]*\\)-\\([0-9]*\\)/\\1\\2\\3/' contacts.txt
sed -i 's/(\\([0-9]*\\))\\([0-9]*\\)\\([0-9]*\\)/\\1\\2\\3/' contacts.txt
sed -i 's/\\([0-9]*\\)-\\([0-9]*\\)-\\([0-9]*\\)/\\1\\2\\3/' contacts.txt
sed -i 's/\\([0-9]*\\).\\([0-9]*\\).\\([0-9]*\\)/\\1\\2\\3/' contacts.txt
sed -i 's/\\([0-9]*\\)-\\([0-9]*\\)/\\1\\2/' contacts.txt
```

My telephone numbers now appear much cleaner:

```
TEL;PREF=1;TYPE=voice:2025551212
TEL;PREF=2;TYPE=voice:3035551212
```

The following commands finish the cleanup using Terminal in Ubuntu.

```
sed -i 's/^FN:]/FN://g' contacts.txt
sed -i 's/^[:]*://g' contacts.txt
sed -i 's/\\,\\/:/g' contacts.txt
sed -i 's/\\;/\\/:/g' contacts.txt
sed -i 's/NICKNAME\\/:\\/:/g' contacts.txt
sed -i 's/ORG\\/:\\/:/g' contacts.txt
sed -i 's/TITLE\\/:\\/:/g' contacts.txt
sed -i 's/NOTE\\/:\\/:/g' contacts.txt
```

```
sed -i 's/home\:/\:/g' contacts.txt
sed -i 's/HOME\:/\:/g' contacts.txt
sed -i 's/work\:/\:/g' contacts.txt
sed -i 's/WORK\:/\:/g' contacts.txt
sed -i 's/cell\:/\:/g' contacts.txt
sed -i 's/CELL\:/\:/g' contacts.txt
sed -i 's/INTERNET\:/\:/g' contacts.txt
sed -i 's/TEL\:/\:/g' contacts.txt
sed -i 's/EMAIL\TYPE\=//g' contacts.txt
sed -i 's/ADR\://g' contacts.txt
sed -i 's/main\://g' contacts.txt
sed -i 's/internet\TYPE\=//g' contacts.txt
sed -i 's/TEL\TYPE\=//g' contacts.txt
sed -i 's/TYPE\=pref//g' contacts.txt
sed -i 's/TYPE\=voice//g' contacts.txt
sed -i 's/TYPE\=//g' contacts.txt
sed -i 's/ADR\Pref\=[0-9]//g' contacts.txt
sed -i 's/BDAY\:00\:-00\:-00FN//g' contacts.txt
sed -i 's/PREF\=[0-9]//g' contacts.txt
sed -i 's/ITEM[0-9]\.EMAIL//g' contacts.txt
sed -i 's/CATEGORIES\myContacts//g' contacts.txt
sed -i 's/item[0-9]\.\://g' contacts.txt
sed -i 's/\:\:/\:/g' contacts.txt
sed -i 's/\:\:/\:/g' contacts.txt
sed -i 's/\:\:/\:/g' contacts.txt
sed -i 's/\:\:/\:/2' contacts.txt
```

I now have everything in order on one line, without any unnecessary junk, ready for import. Each of my contact list entries appear as follows.

Doe:John,jdoe@protonmail.com:2025551212:3035551212:1234 Main:Houston:TX:77089:USA:
Privacy Corp:We met at Blackhat

Next, I can import this list into KeePassXC with the following steps:

- Rename contacts.txt to contacts.csv
- KeePassXC > Database > Import > CSV File...
- Label as “Contacts” > Continue > Continue
- Enter Password > Done
- Save as “Contacts.kbdx”

When prompted, apply the following configuration.

Group	Not Present ▼	Notes	Column 2 ▼
Title	Column 1 ▼	TOTP	Not Present ▼
Username	Not Present ▼	Icon	Not Present ▼
Password	Not Present ▼	Last Modified	Not Present ▼
URL	Not Present ▼	Created	Not Present ▼

My contacts are clean and sorted by last name. An individual entry appears as follows.

Title:	Doe:John
Username:	
Password:	<input type="password"/>
URL:	https://example.com
Expires:	2/24/21 5:12 PM
Notes:	jdoe@protonmail.com:2025551212:3035551212:1234 Main:Houston:TX:77089:USA:Privacy Corp:We met at Blackhat

I can now save this database and copy it to my mobile devices for use with Strongbox (iOS) or Keepass2Android Offline (GrapheneOS). I can copy/paste any numbers or email addresses from KeePassXC into email or VOIP calling applications. It is offline and securely encrypted. If the database should get in the wrong hands, it is useless without the decryption password.

It may be easy to scoff at this technique as unnecessary paranoia. You might be right. However, consider two scenarios. I have many clients who have moved to anonymous homes; make calls with anonymous VOIP numbers; and send emails from private accounts. I know all of the details because I set it all up and use this information to contact them. If I placed this all in a Gmail account, it is exposed to Google employees, criminal hackers, and unknown third parties. That is unacceptable.

If you are still not convinced, consider your own details. Would you want me to place your home address, cellular number, email account, and other sensitive content within an online repository which may later share or sell your information? I know I do not want my details exposed, so I protect the integrity of my clients' contacts.

Account Summary

Hopefully you now have an email, calendar, and contacts solution which is private and secure. We should bring absolutely nothing from our past life into our new private life. Once you have new hardware and new accounts for communication, my preference is that you never access the old accounts from your new devices. The previous forwarding strategies are fine, and should work without logging in to your old accounts. This is especially important for mobile devices, and I insist that Google apps are never installed anywhere. This would immediately associate the new device with the old Gmail account, and ruin the isolation created.

I realize that the previous email strategies can seem overwhelming. As stated previously, privacy is a marathon, not a sprint. Each step you take makes you more private and secure. You can always upgrade your strategy once you have an understanding of the basics. You may also tweak pieces of each option and create your own solution. My goal is to simply present numerous ideas to aid in your own execution. Privacy and security are never simply black or white. A single solution is never appropriate for everyone. Take the time to consider your best options for your own situation.

I encourage you to begin visually creating your own email strategy. I often draw diagrams, using pencil and paper, until I have created a workflow that makes most sense for a specific client. This may seem archaic, but the visual representation helps me. My overall strategy has changed considerably since I began this journey. I would anticipate changes to your own plans as your digital life is hardened. I know I will never be completely satisfied with my own methods of paranoia.

Now that you have the basics covered, let's expand our new private computer. Most, if not all, of the following applications and techniques will work on any operating system, but I will always place emphasis on Ubuntu Linux. My goal is to demonstrate that you can replicate practically any task from your Windows or Mac environments within Linux. If you are a Mac user, I will assume you have already installed Brew as previously explained. I assume Linux users are now comfortable with the Terminal environment.

Windows users can download most applications as standard installation files. However, I encourage you to research a package manager called **Chocolatey** (chocolatey.org). It simplifies most software installations into a single command entered in a Command Prompt window. I don't use Windows daily, but if I did, I would rely on Chocolatey for most software installations. It allows you to install software quickly, especially when you need to install many new programs into a host or virtual machine.

VOIP Calling

In the previous chapter, I explained how to configure Twilio and Telnyx for use with Linphone in order to make and receive telephone calls from VOIP numbers. My favorite modification of this strategy is to configure my laptop to act as my primary telephone. You can download the Linphone app from linphone.org and install as you would any other program. On mac, I entered “brew install linphone” within Terminal. On my Ubuntu Linux machine, I conducted the following.

- Navigate to linphone.org/releases/linux/app/ and download the latest version.
- Right-click the file, select “Properties”, “Permissions”, and enable “Allow executing”.
- Double-click the downloaded file to launch. Copy this file to the Desktop if desired.

You may need to reboot Linux before the application will launch. After opening the software, conduct the following for the appropriate service (or both).

Twilio:

- If prompted upon launch of Linphone, choose “Account Assistant”.
- Click “Use a SIP Account”.
- Enter a “Username” of your number, such as “2025551212”.
- Enter a “Display Name” of your telephone number, such as “2025551212”.
- Enter a “SIP Domain” of your full domain which was used in the previous chapter.
- Enter the “Password” you previously created for the credential account.
- Change the “Transport” to “TLS”. If this ever fails, try “UDP” or “TCP”.

Telnyx:

- If prompted upon launch of Linphone, choose “Account Assistant”.
- Click “Use a SIP Account”.
- Enter a “Username” of your number, such as “2025551212”.
- Enter a “Display Name” of your telephone number, such as “2025551212”.
- Enter a “SIP Domain” of sip.telnyx.com.
- Enter the “Password” you previously created for the credential account.
- Change the “Transport” to “TLS”. If this ever fails, try “UDP” or “TCP”.

Your Linphone laptop application can now make calls from the same VOIP numbers which were previously configured for your mobile device. Incoming Twilio and Telnyx calls will ring to whichever device is open.

Secure Communications Applications

In the previous chapter, I explained secure communication applications such as Signal and Wire. Another benefit of these services over traditional SMS text messaging is the ability to install them as desktop applications for use within a traditional computer. Both offer native Windows and Mac apps on their website. For mac, you can enter “brew install signal” and “brew install wire” within Terminal. As expected, Linux requires some additional steps. The following commands are included at inteltechniques.com/EP for easy copy and paste.

- wget -O- <https://updates.signal.org/desktop/apt/keys.asc> | gpg --dearmor > signal-desktop-keyring.gpg
- sudo mv signal-desktop-keyring.gpg /usr/share/keyrings/
- echo 'deb [arch=amd64 signed-by=/usr/share/keyrings/signal-desktop-keyring.gpg] <https://updates.signal.org/desktop/apt> xenial main' | \ sudo tee -a /etc/apt/sources.list.d/signal-xenial.list
- sudo apt update && sudo apt install signal-desktop
- sudo apt install apt-transport-https
- echo "deb [arch=amd64] <https://wire-app.wire.com/linux/debian> stable main" | sudo tee /etc/apt/sources.list.d/wire-desktop.list
- sudo apt update && sudo apt install wire-desktop

After installation, you can log in to any Wire account through the Linux application. Launching Signal presents a QR code which will need scanned with your mobile device. Open Signal on mobile; open “Settings”; click “Linked Devices”; then “Link New Device”. Your device will prompt you to scan the relevant code.

Notes

Applications such as Evernote, OneNote, and Apple’s iCloud Notes are extremely convenient. They also store your sensitive content in an unencrypted state for employees, criminal hackers, and third-party companies to abuse. I never recommend any of these services to clients. Instead, I rely solely on **Standard Notes** (standardnotes.org) for all of my notes and task lists. This service, with free and paid tiers, provides an elegant application for all major platforms, including mobile devices. All notes are end-to-end encrypted with zero-knowledge from the provider. The free plans are sufficient for most users. Notes updated on one device synchronize securely to all other devices. Many of my clients share a single account with multiple family members as a way to keep track of upcoming events and tasks. My notes and outlines for this book were stored completely within Standard Notes at all times. Linux users can download the “app image” and apply the same methods as Linphone on the previous page for installation. Mac users can enter “brew install standard-notes” into Terminal.

Account Access Monitoring

You likely now possess multiple new online accounts associated with email, messaging, VOIP, and domain registration. Hopefully, you provided new usernames, randomly-generated passwords, and secure two-factor authentication. The chance of unauthorized access to these accounts is slim, but never impossible. You should consider occasional monitoring of various access logs. This could identify attempted or successful access into your accounts. Let's walk through a few of the options which have been previously presented.

ProtonMail: Navigate to “Settings” > “Manage Account” > “Security” from within a web browser. The “Session Management” section displays all apps which have accessed your ProtonMail account. This includes mobile apps, ProtonVPN sessions, and the bridge application. If you see anything suspicious, you can revoke the authentication for that instance. The “Authentication Logs” section displays every login attempt through the ProtonMail website. This includes unsuccessful attempts and the IP addresses of the connections. This can identify malicious login attempts from an adversary.

Messaging: If someone attempts to take over your Signal account, you will receive a text message or call to the VOIP number associated with the account. This is not a high risk. Wire sends you an email any time a new device (including web browser) accesses the account. If you ever want to confirm any connected device, navigate to “Settings” > “Devices” within the Wire application.

VOIP: If you use a Google Voice account with 2FA, you are probably secure from outside attacks. However, you can always see the connection logs at <https://myaccount.google.com> by clicking “Security” > “Review security activity”. Unfortunately, neither Twilio or Telynx offer a way to monitor account access. Be sure to enable 2FA on those accounts.

Domain/Host: This may be the most important monitoring option for those who own custom domains and web hosting. Navigate to your “cPanel” dashboard available within your account portal. Click “Contact Information” in the “Preferences” section. Confirm your desired email address and select every option in the “Notify me when...” area. This generates an email any time your account is accessed. This includes website logins, FTP connections, and any other feature which requires credentials. This can identify attempts to access your domain and hosting, which could be devastating.

Consider all of your online accounts and identify those which offer similar monitoring options. If you are targeted by a tech-savvy stalker, these logs can identify any attacks and may provide evidence for law enforcement.

Tor Browser

You may be wondering why I did not mention the Tor Browser (torproject.org) during the previous private web browsing section. 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 Windows, Mac, and Linux. It relies on a hardened version of Firefox and appears similar to a standard browser in many ways. I conducted the following within Terminal to install Tor within Ubuntu.

- `sudo add-apt-repository ppa:micahflee/ppa`
- `sudo apt update`
- `sudo apt install torbrowser-launcher -y`

Mac users can enter “brew install tor-browser” within Terminal.

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 access the site.
- Restricted Content: Some public networks filter internet traffic such as dating websites, social networks, and mature content. My library blocks Craigslist for some reason. Some countries block news or content which contradicts their own agendas. In 2019, Russia was blocking access to ProtonMail. Tor eliminates these roadblocks.

If you anticipate extensive travel to countries which block open internet access, I would configure a pluggable transport within the Tor Browser before travel. I use **Meek**. Meek is an obfuscation layer for Tor designed to evade internet censorship. Traffic is relayed through a third-party server which is difficult to detect and block. More details can be found on the official Tor website at trac.torproject.org/projects/tor/wiki/doc/meek.

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). 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, which is included with premium subscriptions. I can also share data from this account with secure password-protected and encrypted links.

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 **all** 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 big 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 iPhone. I have the fingerprint and face identification options disabled.

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 can't call them later and ask them to delete the 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, 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.

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.

Virtual Machines

Virtual machines (VMs) conduct emulation 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. When finished with these instructions, you will have a “clean” environment with no contamination from other internet usage. You will be able to clone an original VM in minutes and will no longer need to worry about persistent viruses, tracking cookies, or other invasive tactics. We will use virtual machines in order to isolate our sensitive computer usage from the daily driver which gets bombarded with online tracking.

Before creating a virtual machine, you must possess virtual machine software. There are several free and paid programs which allow you to create and execute virtual machines. Premium options such as VMWare offer a free version, but it is extremely limited in function. However, **VirtualBox** (virtualbox.org) is completely free and easy to operate. Volumes could be written about the features and abilities of VirtualBox. I will first explain how to install the application and then ways to configure a virtual machine. At the time of this writing, the following Terminal commands installed VirtualBox to my Ubuntu Linux machine.

- sudo apt update
- sudo apt install virtualbox virtualbox-ext-pack -y

Mac users can enter “brew install virtualbox virtualbox-extension-pack” into Terminal.

The only requirement for VirtualBox to function is a computer that supports virtualization. Any modern Apple product will work without any modification. Most mid-range and high-end Windows computers made within the past five years should have no problem, but may require you to enable virtualization support in the BIOS (Basic Input / Output System) during startup. Netbooks, older machines, and cheap low-end computers will likely give you problems. If you are in doubt about meeting this requirement, search for your model of computer followed by “virtualization” and you should find the answers. The rest of this section will assume that your computer meets this requirement.

In Chapter One, I explained how I recommend Ubuntu Linux as a dedicated host for your desktop operating system. We can also use this same OS within a virtual machine. Either use the same ISO file previously downloaded or repeat the process to obtain the appropriate file. Next, open VirtualBox and click on the button labeled “New”. The following steps should create a new VM appropriate for our needs.

- Provide a name of “Privacy Original”.
- Choose your desired location to save the machine on your host (I chose Documents).
- Select “Linux” as type, “Ubuntu 64-bit” as version, and click “Continue” (or “Next”).
- In the Memory size window, move the slider to select 50% of your system memory.
- Click “Continue” and then “Create”.
- Leave the hard disk file type as “VDI” and click “Continue” (or “Next”).
- Select the default option of “Dynamically allocated” and click “Continue” or “Next”.
- Choose the desired size of your virtual hard drive. If you have a large internal drive, 20GB should be sufficient. If you are limited, you may need to decrease that number.
- Click “Create”.

Your VM has been created, but it will do nothing upon launch. We need to tell it to boot from the ISO file which we previously downloaded. We should also increase the cores. Select your new machine in the menu to the left and complete the following steps.

- Click the “Settings” icon then the “Storage” icon.
- Click the CD icon which displays “Empty” in the left menu.
- Click the small blue circle to the far right in the “Optical Drive” option.
- Select “Choose Virtual Optical Disk File” and select the Ubuntu ISO downloaded.
- Click “System” in the menu then “Processor”.
- Change the “Processor(s)” to half of those available.
- Click “OK” and then “Start” in the main menu.

Your Ubuntu installation process should now start within a new window. You should be booting to the ISO file previously downloaded, which is behaving as if you had placed an Ubuntu install CD into the virtual computer. This is your first virtual machine running on top of your host operating system. We can now finish the installation with the following steps within the VirtualBox window of your Ubuntu installation.

- On the Welcome screen, choose “Install Ubuntu” and select your language.
- Choose “Normal Installation” and check both download options under “Other”.
- Choose “Erase disk and install Ubuntu”.
- Click “Install Now”, “Continue”, choose a location, and click “Continue”.
- Provide a generic name such as “Laptop”, and enter a secure password.
- Confirm your selections, allow the installation to complete, and reboot.
- Provide your password(s), then click “Skip” on the Welcome screen.
- Select “No, don’t send system info”, “Next”, “Next”, and “Done”.
- If you receive a notice about updates, click “Install Now” and allow to reboot.

You now have a functioning virtual machine which contains the basic programs we need to use the internet. By default, it is using your host computer's internet connection, and taking advantage of your host's VPN if you have it connected. Technically, we could start using this machine right away, but the experience would get frustrating. We need to take some additional steps to configure the device for optimum usage. The first step should be to install VirtualBox's Guest Additions software. This will allow us to take advantage of better screen resolution and other conveniences. Conduct the following steps.

- In the VirtualBox Menu, select “Devices” > “Insert Guest Additions CD Image”.
- Click “Run” when the dialogue box pops up and provide your password.
- Allow the process to complete and restart the VM.

You should now have VirtualBox Guest Additions installed. You can test this by resizing the screen. If you make the Ubuntu VM full screen, you should see the overall screen resolution change with it. If this appears to be functioning, you can right-click the CD icon on the desktop and choose “Eject”. If not, double-click the CD icon and choose “Run Software” in the upper right corner to repeat the process. I have occasionally experienced an inability to resize VM windows within VirtualBox with the “Auto-resize Guest Display” greyed out. The following commands within Terminal of the Linux VM should repair. There is no harm running these if you are unsure.

- sudo apt update
- sudo apt install -y build-essential dkms gcc make perl
- sudo rcvboxadd setup
- reboot

Next, we should make some modifications within the VirtualBox program in order to experience better functionality. Shut down the Ubuntu VM by clicking on the down arrow in the upper right and choosing the power button, followed by “Shut down”. In VirtualBox, select your Ubuntu VM and click the “Settings” icon. Next, conduct the following steps.

- In the “General” icon, click on the “Advanced” tab.
- Change “Shared clipboard” and “Drag n’ Drop” to “Bidirectional”.
- In the “Display” icon, change the Video Memory to the maximum.
- Click “OK” to close the settings window and restart your Ubuntu VM.

You should now have a more robust display and copy and paste capabilities. This has improved a lot of function, and now it is time to personalize the machine. I conducted the following on my new VM.

- Click the “nine dots” in the lower left to launch the Applications menu.
- Open Terminal and enter the following commands.
 - gsettings set org.gnome.desktop.background picture-uri “
 - gsettings set org.gnome.desktop.background primary-color 'rgb(66, 81, 100)'
- sudo apt purge -y apport
- sudo apt remove -y popularity-contest
- sudo apt autoremove -y
- Close Terminal and open “Settings” from the Applications menu.
- In the “Settings” menu, click “Notifications” and disable both options.
- Click the “Privacy” option, click “Screen Lock”, and disable all options.
- Click “File History & Trash” then disable the option.
- Click “Diagnostics” then change to “Never”.
- Click the back arrow, click “Power”, and change “Blank Screen” to “Never”.
- Click “Automatic Suspend” and disable the feature, then close all Settings windows.

These changes should create a more private and pleasing environment. It is important to keep the software on this original VM updated. There are different ways to do this, but I will focus on the easiest way within the operating system applications. While we do this, it may be a good time to add some commonly used applications to our Dock. Conduct the following steps.

- Click the “nine dots” to launch the Applications Menu.
- Type “Terminal” into the search field.
- Right-click on the application and select “Add to Favorites”.
- Type “Software” into the search field.
- Right-click on “Software Updater”.
- Select “Add to Favorites”.
- Press escape until all windows are gone.
- Launch the Software Updater icon from the Dock.
- Click “Install Now” and allow the updates to complete.

You now have Terminal and Software Updater in your Dock for easy access. You can also right-click on any undesired icons within the dock and easily remove them. Check for updates weekly and keep your original copy ready for usage. This brings us to a conversation about the term “Original”. Ideally, you will keep a copy of this VM clean and free of any internet usage or contamination. There are two ways to achieve this, and both have unique benefits. First, let’s discuss Snapshots.

Virtual Machine Snapshots

A great feature of virtual machines is the use of Snapshots. These “frozen” moments in time allow you to revert to an original configuration or preserve an optimal setup. Most users install the virtual machine as previously detailed, and then immediately create a snapshot of the unused environment. When your virtual machine eventually becomes contaminated with remnants of other investigations, or you accidentally remove or break a feature, you can simply revert to the previously created snapshot and eliminate the need to ever reinstall. Consider how you might use snapshots, as detailed in the following pages.

Upon creation of a new Ubuntu virtual machine, apply all updates as previously mentioned. Completely shut down the machine and open the Snapshots option within your virtual machine software. Create a new snapshot and title it “Original”. Use this machine for a single investigation, and export all evidence to an external USB device, such as a flash drive. You can then “restore” the Original snapshot, and it overwrites any changes made during the previous investigation. Upon reboot, all history and evidence is eliminated. This ensures that you never contaminate one virtual machine with another. When there are substantial updates available for Ubuntu, you can load the default configuration, and apply all updates. You can then shut the machine down completely and delete the Original snapshot, without saving it, and create a new snapshot titled Original. This new snapshot possesses all of the updates. If using this technique, I usually delete and create a new snapshot weekly. Conduct the following.

- Completely shut down the Virtual Machine.
- In the VirtualBox Menu, click on the Snapshots button in the upper right.
- Click on the blue camera icon to “take a snapshot”.
- Create a name for the snapshot, such as “New Install”, and click OK.

You can now use your virtual machine as normal. If you ever want to revert to the exact state of the machine that existed at the time of the snapshot, follow these instructions.

- Completely shut down the Virtual Machine.
- In the VirtualBox Menu, click on the Snapshots button in the upper right.
- Select the desired snapshot to apply.
- Click on the blue camera icon with arrow to “restore snapshot”.
- Deny the option to save the current data, and click Restore.

If you want to remove a snapshot, click the icon with a red X. This will remove data files to eliminate wasted space, but you cannot restore to that image once removed. It will not impact the current machine state. Many users remove old, redundant snapshots after creating newer clean machines. Today, I rarely use snapshots and rely on cloned machines, as explained next.

Virtual Machine Clones and Exports

If you ever want to preserve a specific state of Ubuntu, you can clone an entire session. As stated previously, I prefer clones over snapshots. I create an exact replica of my Original VM for every scenario, and never use Snapshots within these unique VMs. For clarity, consider my routine for sensitive investigations, which takes advantage of the “Clone” option within VirtualBox.

- Launch the Original virtual machine weekly to apply updates or global changes, then close the VM.
- In the VirtualBox menu, right-click on the Original VM and select “Clone”.
- Create a new name such as “Investigation”.
- Click “Continue” (or “Next”) then “Clone”.

This creates an identical copy of the VM ready for my online investigation. I have no worries of contaminating my Original VM or any other copies. I now have a second virtual machine which I can launch when I want a secure operating system which can be used for the next investigation. Since I never use the Original machine to surf the web, conduct searches on Google, or buy products on Amazon, there are virtually no trackers other than those issued by the sites visited during my investigation. Each clone is clean and unused. If desired, I can preserve an exact copy of my cloned machine’s environment for future use with an export. The following steps generate a single file which represents the current state of a VM.

- Shut down the active VM.
- In the VirtualBox menu, select “File” then “Export Appliance”.
- Select the desired machine and click “Continue”.
- Choose your storage location and file name, click “Continue”, then “Export”.

This creates a single large file which can be archived for future use. Choosing the “Import Appliance” menu option allows you to recreate the virtual machine exactly as it existed when the export was created. I find this useful when I want to preserve a machine but do not need it immediately available within my VirtualBox menu. I archive exported copies of prior investigations in order to return to them if necessary. In 2020, I was involved in a civil suit on behalf of a client. The other party insisted on their own copy of my investigative computer in order to conduct their own forensics on my process. I was able to issue the exported file without being required to hand over any hardware. I know online investigations exceed the scope of this book, but preparation for these types of scenarios makes us all more private and secure.

Virtual Machine Troubleshooting

I wish I could say that every reader will be able to easily build virtual machines on any computer. This is simply not the case. While most computers are capable of virtual machine usage, many demand slight modifications in order to allow virtualization. Let's take a look at the most common errors presented by VirtualBox upon launch of a VM.

VT-x is disabled: Any version of this error is the most common reason your VMs will not start. This indicates that the processor of your computer either does not support virtualization or the feature is not enabled. The fix for this varies by brand of machine and processor. Immediately after the computer is turned on, before the operating system starts, enter the BIOS of the machine. This is usually accomplished by pressing delete, F2, F10, or another designated key right away until a BIOS menu appears.

Once in the BIOS, you can navigate through the menu via keyboard. With many Intel processors, you can open the “Advanced” tab and set the “Virtualization (VT-x)” to “Enable”. For AMD processors, open the “M.I.T.” tab, “Advanced Frequency” settings, “Advanced Core” settings, and then set the “SVM Mode” to “Enable”. If none of these options appear, conduct an online search of the model of your computer followed by “virtualization” for instructions.

VT-x is not available: This is usually isolated to Windows 10 machines. Navigate to the Windows Control Panel and open “Programs and Features”. Click “Turn Windows features on or off” and uncheck all “Hyper-V” features. Click “OK” and reboot. If the Hyper-V option is not enabled, enable Hyper-V, restart the computer, disable Hyper-V, and reboot again. Attempt to start your VM with these new settings.

This may seem backwards, but it makes sense. Previous versions of VirtualBox cannot run if you are using “Hyper-V” in Windows. Basically, both systems try to get exclusive access to the virtualization capabilities of the processor. Hyper-V within Windows receives the access first and impedes VirtualBox from the capabilities. The latest version of VirtualBox attempts to correct this. If the previous setting did not help, try to re-enable all of the Hyper-V options within Windows, reboot, and try to boot your VM again.

If you are still experiencing problems, read the troubleshooting chapter of the VirtualBox manual at virtualbox.org/manual/ch12.html. Expand any errors received and search the provided error codes to identify further solutions.

Virtual Machine Usage

Your Original VM should only be used to install new software and apply updates. It should never be used for online browsing or research. I launch my Original once a week, apply all updates, and close it. I can then use this Original to create a clean and updated virtual machine within minutes. Next, I outline some of my uses for virtual machines. **If you are using a Linux host, this is all likely overkill.** If you are using Windows with a stock browser, VMs offer a lot of protection.

Banking: I keep a VM designated for anything associated with financial transactions. This includes online bill pay, employee payroll, and investment accounts. This way, I know that the VM is free of any viruses or malicious applications. Since it is never used outside of banking, online tracking is minimal.

Shopping: I confess that I rely on Amazon for many things. I place an order at least once a week. When I do, I boot into my VM designated for online shopping. This VM is never used with any email, social networks, or banking accounts. Furthermore, the entire VM is never associated to my true name. It is only used for ordering items with an alias. This way, I know that Amazon never learns my name or identifies any online browsing history.

Research: I conduct a lot of investigations. In my book Open Source Intelligence Techniques, 8th Edition, I explain how I rely on numerous VMs. Every time I need to research something or someone, I clone my Original VM and open the clone. When finished, I either destroy the clone or export it for archiving. This way, each investigation possesses no contamination from other research.

Sensitive Consultations: When a client needs extreme privacy, I always communicate through a Linux VM which has never been used anywhere else. This is likely overkill, but I justify the paranoia. When communicating through Wire via text through this VM, I know there are no malicious programs, cookies, or other invasive software compromising the communication.

If you want to go the extra mile in achieving extreme privacy, I encourage you to understand virtual machine usage, and build VMs ready for cloning. At any given time, I have no fewer than five VMs ready for action. While most of my VMs are based on Linux, you can replicate these steps with a Windows machine. You will need installation media, such as a Microsoft Windows ISO file, and a valid license. Alternatively, you can download pre-built Windows VMs provided by Microsoft from <https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>. These machines can only be used for 90 days, but re-importing the downloaded file resets the clock. Expect annoying licensing notices throughout usage, but these machines are completely legal.

Live USB Operating Systems

A live USB operating system allows you to boot most computers directly from a USB flash drive containing a full operating system which does not rely on any other software from the installed hard drive. They can either be “persistent” with capabilities of writing and storing changes or “static” which do not allow modifications between uses. For our purposes, we want an operating system which does not store any changes and boots without leaving any traces on the USB drive or the computer being used. TAILS is the perfect product for this.

TAILS, an acronym for The Amnesic Incognito Live System, is a security-focused Debian-based Linux distribution aimed at preserving privacy and anonymity. When booted, all incoming and outgoing connections are forced through the Tor network, which was explained earlier. The system is designed to leave no digital footprint.

In a perfect scenario, a USB drive is inserted into a computer which is turned off. When booted, the USB device is chosen and only software from the removable device is presented. You should see an entire operating system which “forgets” all of your activity when shut down. A VPN is not required since your traffic is going through Tor. It includes a web browser and productivity tools by default. Before explaining how to create your own TAILS USB device, consider some reasons why it could be vital to your own situation.

Contaminated Machines: If you only have access to a single community computer, you have no way of knowing the history of viruses, spyware, and malware which has infected it. TAILS bypasses the hard drive and prevents unnecessary risk.

Network Monitoring: TAILS allows people to use the Internet anonymously and circumvent censorship. This includes networks which block specific websites. Journalists abroad often rely on this product when safely reporting issues back to their home countries.

Tech-Savvy Snooping: This is the main reason I send TAILS USB drives to potential clients. Many victims being held against their will only have access to computers and devices which possess software allowing their captors to see everything they do. I have met victims who had remote monitoring apps on their phones and keyloggers on their laptops. TAILS eliminates threats from any invasive software installed in order to eavesdrop on someone. I never want a potential client to communicate with me about an abusive situation if there is a chance the abuser can see the conversation.

Now that you have an idea of the benefits of TAILS, let’s create a bootable USB device. The following steps download the required software and “flash” it to a USB drive.

- Navigate to tails.boum.org/install/download.
- Click the “Download” option.
- Save the “img” file on your computer.
- If desired, verify the authenticity of the download with the optional extension.
- Navigate to <https://www.balena.io/etcher>.
- Download and install the program version appropriate for your OS.
- Insert a USB 3.0 or higher flash drive into your computer.
- Launch BalenaEtcher.
- Click “Select image”.
- Select the TAILS img file previously downloaded.
- In BalenaEtcher, click “Select target”.
- Carefully select the USB drive inserted (contents will be erased) and click “Continue”.
- Click “Flash” to begin the process.

When complete, you now possess a TAILS live USB. Insert it into a computer and turn it on. If the computer boots to the internal operating system, such as Windows or Mac, the machine’s BIOS needs to be told to boot from the USB. The moment you turn on the device, look for any text such as “Setup” or “Boot” options. Press the key which is displayed for this option, such as CMD, F1, F2, F10, F12, or Del. This should present a minimal menu which allows you to choose the USB device instead of the internal hard drive. TAILS should detect any ethernet or Wi-Fi hardware and allow you to connect to the internet through Tor. If you experience any issues, navigate to tails.boum.org/doc.

These steps could be replicated with other operating systems such as Ubuntu, Mint, and even Windows 10. While I encourage you to explore other Linux options, I never recommend Windows bootable drives. You simply cannot stop Microsoft from collecting data about your usage every time you boot the machine. If you have a need for a secondary Windows installation, I encourage you to create one as a virtual machine, as previously explained.

If desired, you could create a Linux boot USB with persistent storage. This would allow you to save data during usage instead of wiping out all changes during shutdown. I never recommend this unless you have a specific need for it. A big advantage of TAILS is the ability to remove all evidence when finished. Adding persistence is a slippery slope toward possessing sensitive data in an insecure format. If you desire an alternative Linux operating system which stores changes, consider a dual-boot laptop. This would allow you to choose from two or more operating systems upon boot. There are ample tutorials online which explain this process for various models of computers.

RSS Feeds

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) for Mac and **FeedReeder** (jangernert.github.io/FeedReader) for Linux, I will provide the demonstration here using **Thunderbird** (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 krebsonsecurity.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://krebsonsecurity.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 krebsonsecurity.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 own blog address of <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). 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) 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. My favorite way to use RSS is with Reddit. I don’t like going to the Reddit website due to the overall negative and toxic environment, plus dozens of trackers being forced to my browser, but I want to stay updated on the content. The following RSS feeds should help explain my usage.

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. If you have an interest in this tactic, please listen to episode 172 of my podcast which explains more. Figure 3.05 displays the folders, feeds, and content within my RSS client.

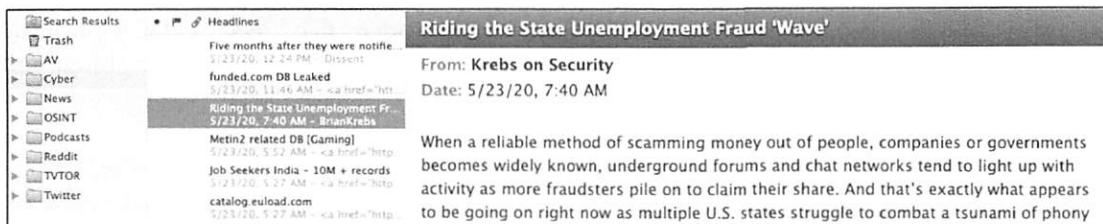


Figure 3.05: An RSS reader application with folders and feeds.

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 VeraCrypt container, 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.

I realize that most readers of this book will not apply all of the strategies presented here. It can be quite overwhelming to tackle all of this at once. I hope you return to this chapter as you progress through your privacy journey. Whenever you have a thirst to add something new to your arsenal, these topics may scratch that itch.

Linux Configuration Backup

Once you have a Linux machine configured exactly as you like it, you should make a backup. This was already briefly discussed in Chapter One, but I believe we need to dive deeper into this important action now. If you ever need to rebuild the operating system due to a hard drive crash, interrupted update, or corrupt data, you do not want to reconfigure all of your settings. Creating an occasional backup of your Home folder ensures you have everything you need for a quick restoration. The following is my protocol, but you may want to tweak things.

- Open the Ubuntu Applications menu and search for “backups”.
- Launch the Backups application and click “Create My First backup”.
- Click “Forward” and select “Local Folder” under “Storage Location”.
- Click “Choose Folder” and select an external drive or flash drive.
- Click “Forward” and password-protect your backup.
- Click “Forward” and allow the process to complete.

If disaster strikes, you may need to reinstall Linux someday. If this happens, be sure to replicate the same username during installation. Conduct the following after installation.

- Open the Backups application and select the “Restore” tab.
- Click the upper menu and select “Preferences”.
- Click “Location” then “Choose Folder”.
- Browse to the backup files present on your external drive.
- Close the open menu windows.
- Drag and select all files and click “Restore”.

This should place all of your configuration files back in your home directory. When you reinstall your software applications, they should identify the files and import any custom configurations. This is never perfect, but should save many headaches. Note that I do not store my documents within the Home folder of Linux. As explained previously, I create a VeraCrypt volume for all important data. This way, my Linux system backups are minimal and fast. I only need the various configuration files which store all of my settings.

If you have the perfect Linux installation with all programs configured as you like them, you might consider a clone of the system. This creates a series of files which can be used to restore your entire system, including all files and structure, exactly as it appeared at the time of cloning. I recommend **Clonezilla** (clonezilla.org) for this purpose. Usage of this tool requires a basic understanding of bootable USB devices and secondary storage drives. Full details are available on their website and do not need repeated here. Use extreme caution with cloning, as it is easy to select the wrong drive and wipe out all contents.

Typical Client Configuration

This is another overwhelming chapter for many readers. The following is the most common actions I take on behalf of a new client seeking extreme privacy.

- Issue a new Ubuntu Linux Laptop.
- Install KeePassXC and explain password manager usage.
- Install Authy and explain Two-Factor Authentication (2FA).
- Issue a YubiKey hardware 2FA USB device.
- Install and configure VeraCrypt and containers.
- Establish a backup protocol and storage solution.
- Harden Firefox for secure and private web browsing.
- Apply DNS settings within Ubuntu.
- Install and configure ProtonVPN on the laptop.
- Create and configure a ProtonMail account with alias addresses and folders.
- Forward email from previous providers to ProtonMail.
- Create and configure SimpleLogin email masking.
- Create and configure a custom domain name.
- Attach new domain name to ProtonMail account.
- Create an offline email archiving solution then delete email from insecure providers.
- Install Linphone and configure home VOIP telephone numbers.
- Install and configure Signal and Wire on the laptop.
- Install and configure Standard Notes on the laptop.
- Install and configure VirtualBox and multiple VMs on the laptop.
- Create a Linux system backup strategy and storage solution.

You can never have privacy unless you possess secure digital devices and connections. This chapter is the backbone for all of the upcoming work you will complete in order to become invisible. As a final note, please remember that technology changes quickly and often. The exact digital tutorials explained in this book ~~may~~ will become inaccurate over time. If you encounter differences during your replication of the steps, online research of the topic should quickly identify new solutions. Later in the book, I present the next level of digital strategies.

CHAPTER FOUR

HOME NETWORK

You are likely no stranger to the importance of virtual private network (VPN) applications 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. It can be used to document your location and track you through every website you visit. Hopefully, you have already included a VPN as part of your privacy strategy. This secures your internet connection and anonymizes your activity online from any device which you have properly configured the VPN application. What happens if the VPN app crashes? What about network connections which cannot take advantage of a standard VPN application?

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 that 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 virtual private network 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 chapter completely before taking any action within your own home network. Throughout this chapter, I will be demonstrating ProtonVPN as my chosen VPN for the configurations. I have found this to be the most private and stable VPN

for router-based installs with automatic reconnections and great speed. This will be explained in more detail later. However, practically any reputable VPN provider could be used within these tutorials.

The goal of this chapter is to create an instance of a single pfSense firewall, which will be the only device in your home that 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 device in your home will ever know the IP address from your ISP. Please note that this chapter has appeared in my other books on privacy and security. However, there are many modifications to this tutorial, and they should replace any previous writings. I firmly insist that every client of mine who is living anonymously possesses this setup. Below 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 quickly associates your Apple account with your home address. A home firewall prevents Apple from ever knowing your true details.
- **Laptops:** Whether 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 chapter.
- **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.

Before discussing the software, I should mention hardware. In order to take full advantage of the bandwidth available through your VPN within a router, your hardware device needs to have a powerful processor, ample RAM, and a solid-state drive (SSD). This firewall is basically an entire computer. You could repurpose a desktop into a pfSense 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 highly recommend a custom **Protectli Vault**, which was created for this purpose.

The unit which I provide to most clients is the \$300 4-port FW4B (amzn.to/31jMzlk). The 2-port FW2B (amzn.to/2NRIfpA) and 6-port FW6B (amzn.to/3lPBaCo) versions would also work great, but I place focus on the most generally applicable model available. Always consider your internet speed before deciding. If you have gigabit internet, a VPN which supports such high speeds, and three kids downloading videos all day, you will want a 6-port Vault which offers faster VPN performance. The 2-port and 4-port models can only handle VPN speeds up to 200-250 mbps, which is typically sufficient for most clients. I have internet speeds less than 200 mbps, so I also use the 4-port FW4B. Whatever you choose, always ensure that your device has a CPU that supports AES-NI (these all do).

I interviewed the CEO of Protectli, on my podcast in 2017 and learned about his company when I was looking for the most appropriate solution to my home router needs. These 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. The model that I chose for testing contained 4GB of RAM and a 32GB MSATA solid-state drive. I have had a Protectli box running almost non-stop for four years.

The following instructions walk you through the entire installation and configuration of a pfSense firewall with a VPN in kill switch mode on this specific device. 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. These instructions were replicated on the currently available latest stable version of pfSense, 2.5.0. Later versions may display minor differences, but the principles of this setup should apply to future releases. 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.

Regardless of whether you have adopted the privacy and security strategies throughout this book, I recommend that you seriously consider the tutorials in this chapter. 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 cheap VPN application is not sufficient. We need stable protection and a backup plan if a VPN connection should fail. This chapter solves these issues.

The content here is presented in several phases. I recommend practicing on your device as you go through these, without connecting it to the internet. 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. **Many readers skip this chapter until they are ready to dive into the technical world of configuring a home firewall.** At the end of this section, I present a page on my website which allows you to download custom configuration scripts which simplify the entire process.

Phase One: Installation: Install the firewall software

The following steps download and configure pfSense onto a USB device.

- Navigate to www.pfsense.org/download.
- Choose “Architecture: AMD64”, “Installer: USB Memstick Installer”, “Console: VGA”, and “Mirror: New York”.
- 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-2.4.5-amd64.img.
- Download and install **Etcher** from <https://www.balena.io/etcher/>.
- 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.

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.

Follow all default installation options, which should require you to strike the enter key several times. After installation is complete, remove the USB flash drive, monitor, and keyboard from the firewall. Connect a computer without internet access via an ethernet cable to the LAN port of the firewall. Navigate to 192.168.1.1 within a web browser and log in with the default username of “admin” and password of “pfsense”. Ignore any warnings about a certificate and click “Advanced” to allow the page to load. Accept all defaults within the setup process with “Next”. Create a secure password when prompted. Click the various demands for “Next”, “Close”, and “Finish” until you are at the home screen.

Note: If your Vault does not recognize the USB device and cannot boot into an operating system, you must enter the BIOS of the device and configure it to boot from USB. The procedure for this is different on any machine, but the Protectli Vault is fairly straight-forward.

- Turn on the device and immediately press F11 on the keyboard repeatedly.
- If the USB device is visible on the monitor attached to the Vault, select it.
- If USB device is not visible, 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.

Phase Two: Activate Ports (Optional)

If you purchased a 4-port or 6-port option, you can activate these ports at this time by configuring the following changes. If you purchased the 2-port FW2B, skip this page.

- Navigate to “Interfaces” then “Assignments”.
- Click the “Add” option next to each empty port, which will add one port at a time.
- Repeat until all ports have been added and “Add” is no longer available.
- Save your changes.
- Click through each new option (“Interfaces” > “Opt1”/“Opt2”/etc.).
- Enable each port by checking the first box, and saving your changes each time.
- Navigate to “Interfaces” then “Assignments” to continue to each “Opt” option.
- When finished with all of them, apply the changes in the upper right.
- Navigate to “Interfaces”, “Assignments”, then select “Bridges” in the upper menu.
- Click “Add” to create a new bridge.
- Select the LAN option as well as each port that was added with ctrl-click or cmd-click.
- Provide a description, such as “bridge”, and click “Save”.
- Navigate to “Firewall” then “Rules”.
- Click each port (Opt1, Opt2, etc.) and click the “Add” button (up arrow) for each.
- Change the “Protocol” to “Any”.
- Click “Save” after each port is modified.
- Apply changes in upper-right after all ports have been added.
- Navigate to “Interfaces” then “Assignments”.
- Click “Add” next to “BRIDGE0” and click “Save”.
- Click on the bridge, which may be labeled as “Opt3” or “Opt5”.
- Enable the interface and change the description to “bridge”.
- Click “Save” and then “Apply Changes”.
- Navigate to “Firewall” then “Rules”.
- Click on “Bridge” then click the “Add” button (up arrow).
- Change the “Protocol” to “Any” and click “Save”.
- Apply changes in upper-right.

Please note that enabling these ports allows you to attach additional devices to your firewall. However, you still need to have an active ethernet device plugged into the LAN port of the firewall in order for the additional ports to function. 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. Overall, the LAN port is the primary connection and should always be in use.

Phase Three: Configure VPN Settings

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 only 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 present an option for ProtonVPN during this phase, but you could replicate these steps with most VPN providers. It is vital to choose a stable VPN provider with good speed and reputable privacy policies. ProtonVPN offers a higher level of privacy and security (in my opinion), but costs a bit more than other popular providers. It also requires a few extra steps during configuration. ProtonVPN has less users, which means less people associated with each IP address. This could lead to less restrictions on sites which block VPNs and fewer captchas when visiting websites with DDOS protections. Most users will see no difference in the usage of one provider versus the other. Please check inteltechniques.com/vpn.html for the latest information about suggested VPN providers. **Most clients' firewalls use ProtonVPN as the VPN service.**

These instructions assume you possess VPN service through ProtonVPN. First, we need to download their certificate, which involves a few extra steps. First, log in to your ProtonVPN account and navigate to <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” > “Cert Manager” > “CAs” and click “Add”.
- Change “Descriptive name” to “VPN”.
- Change “Method” to “Import an existing Certificate Authority”.
- Select and copy all text from “----BEGIN CERTIFICATE----” through “----END CERTIFICATE----” within the previously downloaded ProtonVPN certificate.
- Paste this text into the “Certificate Data” box within pfSense and click “Save”.
- Navigate to “VPN” > “OpenVPN” > “Clients” and click “Add” in the lower-right.
- Confirm “Server Mode” is “Peer to Peer (SSL/TLS)”; “Protocol” is “UDP on IPv4 Only”; “Device Mode” is “Tun - Layer 3 Tunnel Mode”; and “Interface” is “WAN”.
- Enter a “Server Host or Address” of “us.protonvpn.com” (for U.S. users).
- Confirm a “Server port” of “1194” and add a “Description” of “ProtonVPN”.
- Within “User Authentication Settings”, provide your ProtonVPN “OpenVPN / IKEv2 username” credentials which are available in the “Account” section of your ProtonVPN online dashboard. These will be different than your credentials to log in to the ProtonVPN application, and are designated for this purpose.
- Enable “TLS Configuration: Use a TLS key”.
- Disable “Automatically generate a TLS Key”.
- Copy the text from “----BEGIN OpenVPN Static key V1----” through “----END OpenVPN Static key V1----” inside the downloaded ProtonVPN certificate.
- Paste this text into the “TLS Key” box within pfSense.
- Confirm “TLS Key Usage Mode” is “TLS Authentication”.
- Confirm “Peer Certificate Authority” is the “VPN” option created earlier.
- Confirm “Client Certificate” is “None (Username and/or Password required)”.
- Enable “Data Encryption Negotiation”.
- Within “Encryption Algorithm”, add “AES-256-CBC (256 bit key, 128 bit block)” by clicking it, then remove (click) any others inside the box to the right.
- Change “Auth digest algorithm” to “SHA512 (512-bit)”.
- Change “Topology” to “Subnet - One IP address per client in a common subnet”.
- Under “Advanced Configuration”, enter the following within “Custom Options”:


```
tun-mtu 1500;
tun-mtu-extra 32;
mssfix 1450;
persist-key;
persist-tun;
reneg-sec 0;
remote-cert-tls server;
pull;
```
- Change “Gateway Creation” to “IPv4 only”.

- Change “Verbosity level” to “3 (recommended)” and click “Save”.
- 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, OPT4, or OPT6. Click on this new name, which should present the configuration for this interface. Modify the following.

- Enable “Enable Interface”.
- Provide a “Description” of “OVPNC”.
- 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”.
- Change the “Interface” option of “WAN” to “OVPNC” and click “Save”.
- 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”.
- Change the “Interface” option of “WAN” to “OVPNC”.
- Click “Save” then “Apply Changes”.

This phase tells your firewall to route the internet traffic from your various devices through the VPN which you configured on the firewall. This ensures that all of your devices ONLY connect through a VPN, 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, and e-book readers. 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 network.

Your firewall should now automatically connect to ProtonVPN upon boot. This means all of your internet traffic from any 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 “OVPNC_VPNV4”.
- Click “Save” then “Apply Changes”.
- Click the “Disable” icon next to “Default allow LAN IPv6 to any rule”.
- Click “Apply Changes”.
- Navigate to “System” > “Advanced” > “Miscellaneous”.
- Enable “State Killing on Gateway Failure” and “Skip rules when gateway is down”.
- Click “Save”.

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 completely 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 will 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.** Pressing it again reboots the device. **Never hold the power button down longer than a second unless your device is locked-up or not responsive.**

It is time to test our connections. Connect your internet access (cable modem, DSL, etc.) to the WAN port of the pfSense device. Click the pfSense logo in the upper-left to return to the home page of the dashboard. It should now display a WAN IP address in the Interfaces section. Once you have internet access connected to your firewall, navigate to “Status” > “OpenVPN”. If Status doesn’t 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 ProtonVPN masking your IP address from any sites you visit. We will test this later. If you ever want to start over, navigate to “Diagnostics” > “Factory Defaults” to reload the firewall without any modifications.

Phase Four: Prevent DNS leakage

The previous steps force the firewall to use your VPN interface as the default gateway. This means only the VPN can serve web pages, and not the raw internet connection delivering internet access to the device. However, your ISP's DNS servers are possibly still being used. DNS is the technology which translates domain names into the IP addresses needed to complete the connection. Using the default DNS servers from your ISP would tell your ISP every website that you visit, but they could not see the content. It is possible that your VPN provider is acting as a DNS server, which may be acceptable.

Personally, I choose to use a third-party DNS provider in order to have another layer of privacy. My VPN provider is delivering my internet access and content, but a third-party DNS can look up the requests to provide the content to the VPN. This takes away a bit of knowledge about my internet browsing from the VPN company, but not much. Since we are seeking extreme privacy, I believe this extra step is justified. Choosing an alternative DNS provider will also allow us to encrypt our DNS traffic.

Many DNS providers do not allow encrypted connections, so I will use one that does. I chose to make Cloudflare my firewall DNS provider. They are not perfect, and have financial motives for their huge company, but they are better than most of the alternatives, such as Google. I chose Cloudflare because they are one of the few DNS providers which provide encrypted DNS, promise to destroy connection logs after 24 hours, and has been independently audited by KPMG. They also allow us to appear somewhat “normal” while relying on their protections. Using other niche privacy-themed DNS providers can make us stick out as unique. Navigate back to the pfSense Dashboard and conduct the following to change the DNS servers to Cloudflare or any other desired service.

- Navigate to “System” > “General Setup”.
- Add 1.1.1.1 as a DNS server and choose the “WAN_DHCP-wan” interface.
- Click “Add DNS Server”.
- Add 1.0.0.1 as a DNS server and choose the “WAN_DHCP-wan” interface.
- Disable “DNS server override”.
- Change “DNS Resolution Behavior” to “Use remote DNS server, ignore local DNS”.
- Click “Save”.

You may notice that your VPN provider is still acting as your DNS server. This is common and is likely a service to protect you from your own ISP eavesdropping on your traffic. However, I insist on the third-party option. In order to truly force pfSense to allow the third-party DNS and not rely back on the VPN provider, we can conduct the following.

- Navigate to “Services” > “DNS Resolver” > “General Settings”.
- Enable “Enable DNS Resolver”.
- Within “Outgoing Network Interfaces”, select “OVPNC”.
- Enable “DNS Query Forwarding”.
- Within “Custom Options”, add the following text.

```
server:  
forward-zone:  
name: “.”  
forward-ssl-upstream: yes  
forward-addr: 1.1.1.1@853  
forward-addr: 1.0.0.1@853
```
- Click “Save” and “Apply Changes”.
- Reboot the firewall through “Diagnostics” and “Reboot”.

Return to the Dashboard and ensure that the only DNS servers listed are those desired. Navigate to <https://whatismyipaddress.com> and ensure that your VPN IP address is shown. Conduct an Extended Test at <https://dnsleaktest.com> and ensure that only the chosen DNS provider details are shown.

Why is this important? If you have configured your firewall correctly, all DNS requests from your devices will be handled by Cloudflare. By enabling DNS over TLS, the requests are encrypted and your ISP will only see that you are connecting to a DNS provider without being able to see the requests themselves. In other words, your ISP will not know which websites you visit, only the amount of data used to generate the content.

There are many DNS server options. While I chose to use Cloudflare, you could easily pick another option such as OpenDNS. I chose Cloudflare in order to take advantage of the encrypted option and eliminate any extra potential data leaks. Many VPNs use their own DNS servers, but some leak to your internet service provider. The most vital concern here is to occasionally test for DNS leaks at <https://dnsleaktest.com>.

Overall, I do not like placing all of my eggs (visited websites) in one basket (VPN provider). Isolating these tasks provides another layer of privacy and security. If you would like more information about DNS as it relates to privacy, please listen to my podcast on this topic titled, “124-Does DNS Matter?” on my website at inteltechniques.com/podcast.html.

Do not take the choice of VPN and DNS providers lightly. Do your homework and make the best decision for your needs.

Phase Five: Enable AES-NI CPU Crypto & PowerD

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 drop-down menu.

Next, 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. Navigate to the following to activate this setting.

“System” > “Advanced” > “Miscellaneous” > “Power Savings” > Enable “PowerD”

Click “Save” when finished. Please note that the configuration files hosted on my site, which are explained in a moment, already include the activation of AES-NI and PowerD, as well as all previous standard configurations. Overall, manually configuring everything in this chapter whenever possible is best. However, backup scripts may save you time when you need immediate access to the internet and your installation has become corrupt. Know all of your options, and understand the technology which makes everything function.

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. Mine has saved me from many rebuilds.

Phase Six: Disable Annoyances and Test Device

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, disable “SMTP Notifications”.
- In the “Sounds” section, check the “Disable startup/shutdown beep” option.
- Click “Save”.

You should now test your new “kill switch”. 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. Conduct a final test on the following websites and make sure your IP address and DNS server addresses match with what you chose during the setup.

<https://www.dnsleaktest.com/>

<https://browserleaks.com/ip>

<https://www.deviceinfo.me/>

Let’s pause now and reflect on what we have achieved. The pfSense firewall is providing protection between your internet connection and your laptop, which is likely 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. If you never plan to connect other devices, such as a wireless router, tablet, or streaming service, then your setup may be finished. This would be a rare scenario. In a moment, I explain how to introduce Wi-Fi to this configuration. The DNS servers that translate domain names into IP addresses are only those 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.

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 Mac laptop, and a connection to the router is made.

In milliseconds, your computer now has full internet access using your real IP address. Windows computers will start to send data to Microsoft while Mac 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.

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-Netflix.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. Conduct the following.

- 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 in this section to begin the update process.

Finally, one last thing to consider. If you are setting up a new pfSense hardware device, the MAC address of the WAN port has never been used. This unique address will be shared with your internet service provider, which is not a big deal at this point. However, if you were to move to a new home, and take this device with you, the next internet service provider will see this same address. If you have the same provider, it would immediately know that you are the same customer, regardless of the name you provided for this new account. The solution is to either buy a new box when you move, or “spoof” the MAC address with the following steps.

- Navigate to “Interfaces” > “WAN”.
- Provide a random set of numbers matching the pattern provided.

This should be done before connecting the internet connection. This may be overkill for most, if not all readers, but I want you to know your options and risks.

Optional: Choose a Different ProtonVPN Server

Note that I chose “us.protonvpn.com” as my server host. This will automatically connect to a random stable U.S. server regardless of account tier possessed. If you are not in the U.S., or prefer to always select a specific server in a set location, you must choose your desired server at <https://protonvpn.com/vpn-servers>. Let’s assume you are near Texas and want to use only Texas servers. At the ProtonVPN servers website, we see that we can choose from “US-TX#1” through “US-TX#8”. Some have a “P” next to them indicating a server which requires a “Plus” tier account. Next, navigate to <https://mxtoolbox.com/DNSLookup.aspx> and enter the proper structure for each server. As an example, I formatted the first three Texas servers as follows, which each produced the IP address immediately after.

us-tx-01.protonvpn.com = 209.58.147.42

us-tx-02.protonvpn.com = 209.58.147.43

us-tx-03.protonvpn.com = 209.58.147.44

I could place the first IP address in the previously explained “Server Host” field and my firewall would connect to that server each time by default. If desired, you can add any other servers under the “Advanced Configuration” option previously explained. This will issue a random server from specific options upon boot and skip any server which does not respond. This is how I configure my firewall at home. Let’s walk through this entire optional process. **Conduct the following ONLY if you do not want to use a general U.S. server and have a need for specific servers based on location or “Plus” tiers.**

- Identify the IP addresses of the desired servers using the previous instruction.
- Navigate to “VPN” > “OpenVPN” > “Clients”.
- Click the pencil icon next to your configuration to edit.
- Replace “us.protonvpn.com” with the first IP address from your desired servers.
- In the “Advanced Configuration section, scroll to the bottom of the “Custom Options” until you see “pull;”.
- Add the remaining desired server IP addresses on the line immediately after “pull;”, in the format as follows. Click “Save” when finished.

remote 209.58.147.43 1194;

remote 209.58.147.44 1194;

remote-random;

If you have no preference of a specific location, and you are in the U.S., “us.protonvpn.com” is the easiest setting. The optional configuration presented here allows you to only use local servers which support Plus and Visionary speeds if allowed by your subscription. I selected only “Plus” servers in my area and experience minimal captchas and video streaming blocks.

Optional: Choose a Different VPN Provider

This section may seem contradictory to my previous statements about focusing solely on ProtonVPN. While sharing the previous steps with members of the IntelTechniques online video training, I discovered that a lot of people were still using Private Internet Access (PIA) as their VPN provider. They all wanted to know the best updated steps for PIA in the latest version of pfSense. This two-page section was added to the book at the last minute in order to assist people in this same situation. It may also assist with modifications for other VPN providers. Please skip the next two pages if you are using ProtonVPN.

I have already stated that I prefer ProtonVPN over all other VPN providers, but that has not always been the case. I strongly supported PIA before ProtonVPN was stable and PIA was acquired by KAPE. Readers who currently have a PIA membership should not abandon the service while time remains on their accounts. When it expires, I believe you should consider making the switch. I always keep an updated page of my current VPN recommendations and discounted purchase links at inteltechniques.com/vpn.html.

The following abbreviated steps would be used in place of “Phase Three” which was previously presented. Include all other phases in the order specified. Note that I do not include any explanation of each step, but the details previously provided should assist with the understanding of the settings required for this provider. These steps should seem familiar if you practiced during the previous tutorials with some minor modifications required by PIA.

- Download <https://www.privateinternetaccess.com/openvpn/ca.rsa.2048.crt>.
- Open this file in a text editor.
- Navigate to “System” > “Cert Manager” and click “Add” in the lower-right.
- Provide a “Descriptive name”, such as “VPN”.
- Change the “Method” to “Import an existing Certificate Authority”.
- Paste all of the text within the previously downloaded file into “Certificate Data”.
- Click “Save”, navigate to “VPN” > “OpenVPN” > “Clients”, and click “Add”.
- Provide a “Server Host” from <https://privateinternetaccess.com/pages/network>.
- Enter a “Server port” of “1198” and “Description” as “PIA”.
- Provide your PIA credentials under “User Authentication”.
- Uncheck “Use a TLS Key”.
- Click all options in the grey box to remove them.
- Click “AES-128-CBC (128-bit)” in the left box to add it to the box on the right.
- Change “Fallback Data” to “AES-128-CBC (128 bit key)”.
- Change “Auth digest algorithm” to “SHA1 (160-bit)”.

- In the “Advanced Configuration” section, enter the following in “custom options”:


```

persist-key
persist-tun
remote-cert-tls server
reneg-sec 0
auth-retry interact
```
- Change “Gateway Creation” to “IPv4 only”.
- Change “Verbosity level” to “3 (recommended)” and click “Save”.
- Select “Interfaces”, click “Assignments”, click “Add”, then click “Save”.
- Click the new option, such as OPT4 or OPT6 then Enable “Enable Interface”.
- Provide a “Description” of “OVPNC” and enable “Block Bogon Networks”.
- Click “Save”, “Apply changes”, then navigate to “Firewall” > “NAT”.
- Click on “Outbound” at the top. For “Outbound NAT Mode,” select “Manual Outbound NAT rule generation”, then 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 - LAN to WAN”.
- Change the “Interface” option of “WAN” to “OVPNC” and click “Save”.
- 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”.
- Change the “Interface” option of “WAN” to “OVPNC”.
- Click “Save”, “Apply Changes”, and 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 “OVPNC_VPNV4”.
- Click “Save” then “Apply Changes”.
- Click the “Disable” icon next to “Default allow LAN IPv6 to any rule”.
- Click “Apply Changes” and navigate to “System” > “Advanced” > “Miscellaneous”.
- Enable “State Killing on Gateway Failure” and “Skip rules when gateway is down”.
- Click “Save” and proceed to Phase Four previously presented.

If you experience any issues, try a different server. The format of each option should be similar to “us-chicago.privacy.network” (Chicago, US). I have witnessed configurations which would not connect until the device was rebooted. Overall, PIA configuration within pfSense has always been tricky. Their website does not always have the latest details and the cryptography is not as robust as ProtonVPN. However, readers with a current PIA subscription should have no trouble using the service within a pfSense firewall and will possess more than adequate protection for our needs. **I maintain active subscriptions with both ProtonVPN and PIA, and have pfSense configuration files ready for each.** If ever needed, I can import a file and quickly switch to a different provider throughout my entire network.

Optional: The “Netflix” Port

This tutorial assumes that you have a 4-port or 6-port Vault, you have already completed the previous instructions including adding the additional ports, and you want to assign one of those ports to connect directly to your internet service provider without any VPN protection. This can be beneficial when you want to stream video from services such as Netflix, but the service is preventing the stream because they are blocking your VPN connection. The following steps reassign the last port on your device to remove the VPN, while still protecting the remaining ports including your Wi-Fi network on the LAN port.

- Within pfSense, navigate to “Interfaces” > “Assignments” > “Bridges”.
- Click the pencil icon to edit the bridge.
- Hold the ctrl (or cmd) key and click to deselect the last “Opt” port (similar to “Opt2” or “Opt 4”).
- Click “Save”.
- Navigate to “Interfaces” > “Assignments”.
- Click on the port which you just removed and configure the following:
 - IPv4 Configuration Type: Static IPv4
 - IPv4 Address: 192.168.2.1
 - /: 24
- Click “Save” then “Apply Changes”.
- Navigate to “Services” > “DHCP Server”.
- Click the same port as previously mentioned.
- Select (check) the “Enable DHCP Server on ...” option.
- Enter the range as “From: 192.168.2.100 To: 192.168.2.150”.
- Click “Save”.
- Navigate to “Firewall” > “NAT” > “Outbound”.
- Click the first “Add” button.
- Change “Address Family” to “IPv4”.
- Add a “Source Network” address of “192.168.2.0”.
- Click “Save” and “Apply Changes”.
- Navigate to “Firewall” > “Rules”.
- Select the same target port as in the previous instructions.
- Click the pencil icon to edit the rule.
- Click “Display Advanced”.
- Change the “Gateway” to “Wan_DHCP...”.
- Click “Save” then “Apply Changes”.

The last port of the firewall should now connect directly through your ISP. This may be labeled OPT2 on a 4-port box or OPT4 on a 6-port box. Typically, it is the port to the far left when looking directly at the ethernet ports on the back of a Protectli Vault. Be careful with this! Anything plugged into that port has no VPN protection.

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 remaining ports, including any Wi-Fi access point connected to your LAN port, still rely on a VPN. Anything connected to those ports are protected.

If desired, you could connect a Wi-Fi router to this newly configured port and allow streaming devices to connect wirelessly. You could replicate the same instructions presented in a moment with the Slate/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 the last port on the firewall, and change the SSID to something similar to "Netflix". Any device which connects wirelessly to this new network will not be protected by a VPN, but will allow access to all streaming 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. In a few pages, I present a diagram of how this might look within your home.

I would feel irresponsible if I closed this section without identifying my personal usage of this technique. Quite simply, I do not enable this feature. I believe exposing my true IP address to any service is too risky for my threat model. However, I also do not subscribe to services such as Netflix, Prime, or Hulu. All of these products monitor your viewing history, location, and schedule. The data is often shared with business partners and affiliates. When adding payment details, home address, and contact details, these services possess a powerful dossier about you.

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.

Custom Configuration Scripts and Purchase Options

When I was updating this chapter for this new edition, I reached out to numerous members of my online video training to test my settings and tell me where I was wrong. During our conversations, we discussed the concerns about offering highly technical tutorials to a mass audience. I have heard from frustrated readers when a required step did not function as intended and served as a roadblock to the remaining instructions. I have also been bombarded with questions about the appropriate models and hardware configurations. I decided it would be best to offer some solutions to all readers in order to eliminate some of the pain.

I have made several custom configuration scripts which can be imported into your own pfSense installation. These scripts contain the exact configurations presented in this chapter up to this point without much manual effort. Each script contains the appropriate VPN settings for U.S. servers for ProtonVPN. Options including the “Netflix” port are provided as separate configuration files. Full details, including direct download links and complete import tutorials, can be found at inteltechniques.com/firewall.

This page also offers all configuration files created during the previous edition of this book; plus, new files specifically made for Private Internet Access (PIA) created with pfSense 2.5.x. I provide these because I have previously endorsed PIA as a viable alternative to ProtonVPN and I know many readers possess three-year memberships. There is nothing (known) wrong with PIA, I simply prefer ProtonVPN due to stronger encryption and a Switzerland legal authority. If choosing a new provider, I believe ProtonVPN is superior. If you already have PIA, use the files configured for that provider.

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 non tech-savvy readers from this privacy strategy. Possessing a firewall within your home network, even without fully understanding the technical details, is better than no protection at all.

Personally, I issue and recommend the 4-port device (amzn.to/31jMzlk) to most clients. It is robust enough for daily usage. I only issue the 6-port option to clients with internet speeds over 250 Mbps and numerous users on the network. 2-port devices should only be considered if internet speeds are below 200 Mbps and less than five devices need to access the device simultaneously. Purchase links can be found at inteltechniques.com/firewall.

While the configuration files on my site were only tested on the three Protectli models cited, I have received feedback from many readers acknowledging that they also worked perfectly on non-Protectli equipment. If you have a device with at least two ethernet ports, these files may work for you. Be sure to test thoroughly and backup any prior configurations.

Optional: Install pfBlockerNG

Prior to 2020, I included a “Pi-hole” within my home network. This small device is a Linux network-level advertisement and internet tracker blocking application, intended for use on a private network. Basically, it is a small box placed between my internet connection and my firewall in order to prevent undesired advertising content from being delivered to my devices. While I believe that Pi-holes are still great for home networks, I have transitioned some clients to pfBlockerNG. This software can be installed directly within your pfSense installation, which eliminates the need for another piece of hardware within your network. The following steps configure this option within your current pfSense build.

- From the pfSense portal, click on “System” then “Package Manager”.
- Click “Available Packages” and search for “pfBlockerNG”.
- Click “Install” next to the “pfBlockerNG-devel” option.
- Click “Confirm” and allow the process to complete.
- When finished, click “Firewall” then “pfBlockerNG”.
- Click “Next” until you are presented with “IP Component Configuration”.
- Choose “WAN” for “Inbound” and “LAN” for “Outbound”, then click “Next”.
- Accept the default webserver configuration, click “Next”, then “Finish”.
- Allow the next page to complete the script download process.

You now possess basic pfBlockerNG protection from invasive ads and tracking. Combined with uBlock Origin, as previously explained, you have a great layer of privacy in both your network and your browser. There are numerous additional feeds which can be enabled, but I typically avoid these. The default protection is sufficient for most. When finished with the pfBlockerNG installation process, conduct the following to fetch any updates.

- Click “Update”, select “Reload” then click “Run”.

The home page of the pfSense portal should now display a new section in the lower right. This window presents statistics regarding the number of intrusions blocked. Navigate to a website such as cnn.com. You should see several white boxes in the place of advertisements. This confirms that your configuration is working. I currently have a love/hate relationship with pfBlockerNG. In 2020, I witnessed conflicts between the default installation options and my protocols for a VPN router. pfBlockerNG stopped working after an update. Furthermore, there are occasions when I want to see a full web page as intended, such as during an online investigation. It is easy to disable uBlock Origin whenever needed, but not as easy to disable pfBlockerNG. I currently do NOT implement pfBlockerNG on my home network. I rely on uBlock Origin and rarely browse the internet from devices other than my laptops. You may have a stronger need for this protection.

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: If your internet provider supplies you with a combination modem and wireless 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. If your ISP provides a combination modem and Wi-Fi router, consider disabling the Wi-Fi feature completely. Connect the modem to the pfSense box, and then connect a wireless access point to the pfSense unit as previously discussed.

Updates: Minor updates to pfSense, such as 2.5.1 and 2.5.2 should not have much impact on your settings. However, major updates such as the eventual 2.6.0 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.

VPN 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 optional “Netflix” port configuration. 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 6-port 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.

Wireless Router

This 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. It is also unrealistic to think that the other occupants of your home will go without Wi-Fi.

By possessing separate devices for your internet connection (cable modem), firewall (pfSense), and wireless router (Wi-Fi), 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.

Regardless of your current scenario, you should consider hiding your wireless network name, officially known as the SSID. Entering your setup utility on the wireless router from a computer connected to the device will allow you to change the broadcast setting to a hidden network. Again, seek the specific instructions for your router online or within the manual. Note that this does not make you invisible. There are plenty of tools which will identify hidden networks. However, this is not common activity conducted by your average neighbor. This will require you to know the specifics of your router when configuring new wireless devices

to access your network. The security and privacy benefits of a hidden network outweigh these rare configuration annoyances.

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 can quickly exceed the scope of this book. Overall, I recommend either DD-WRT or OpenWRT. Let’s dissect each.

DD-WRT (dd-wrt.com): For many years, I configured Wi-Fi routers with DD-WRT as the operating system. I first identified a router which is supported by DD-WRT. These included most versions of the Netgear Nighthawk R7000 AC1900, Linksys WRT3200ACM AC3200, and Asus RT-AC68U AC1900. These can still be found online and in stores. The DD-WRT website explains the process of replacing the stock firmware with this custom open-source software for each router. However, I no longer choose this route.

OpenWRT (openwrt.org): This option is very similar to DD-WRT with a few important differences. Most importantly, there are fewer routers which support this operating system. While OpenWRT allows more granular control than DD-WRT, this can cause unnecessary confusion. This can be beneficial to some while a headache to others. I only recommend flashing your own router with OpenWRT if you have a deep understanding of networking and routers. Instead, I offer a pre-configured option in just a moment.

Tomato: In my previous privacy books, I had high praise for Tomato as the operating system for wireless routers. The specific builds I suggested are no longer updated. While there is still one Tomato project being updated, I no longer endorse it. The previous two options are superior in my opinion.

Whatever device you choose for your Wi-Fi needs, whether stock software or these custom options, remember to disable DHCP (assigns IP addresses) and place your Wi-Fi router into “Access Point” mode if available. If your Wi-Fi router is behind a pfSense firewall, the threat of privacy and security vulnerabilities is much less than if you did not have the firewall protection. Even stock routers without modification are fairly safe as long as they are behind the firewall. Choose the level of privacy and security most appropriate for your situation. The summary at the end of this chapter may help digest all of this information.

There are online providers which will sell you a router pre-configured with your choice of open-source firmware. However, the markup for this relatively easy service is high. I have seen router prices double when they include this free software. I strongly encourage you to research DD-WRT and OpenWRT, identify a supported router, and jump in. Learning the configuration process will help you maintain the device. Alternatively, you could consider a pre-configured “portable” router, such as the device mentioned in the next section. It should simplify all of this.

Portable Routers

A pfSense firewall is essential for a private and secure home, but can be overkill while on the road. However, blindly relying on public Wi-Fi is dangerous. You expose your current IP address (and location) at all times and could be vulnerable to malicious attacks from other devices on the network. This is where a travel router can be a vital piece of hardware for those commonly away from home. I currently provide either a **Slate** (amzn.to/2FYo8i7) or **Beryl** (amzn.to/3bm42xc) portable device to all of my clients who travel frequently, and some use it in their homes at all times as an access point. I explain two specific configurations within the following pages for these scenarios.

The Slate and Beryl 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 book. 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. Since this is technically a travel router, the range will be less than a traditional unit. 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 device.
- Connect an ethernet cable from the router WAN port to the pfSense LAN port.
- Connect a computer or mobile device to the 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, connect to the pfSense portal within your browser.
- Navigate to “Status” > “DHCP Leases” and identify the IP address of the router.
- Navigate to that IP address within your browser.
- Provide a new secure password.
- 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.
- Connect your computer’s Wi-Fi to either SSID on the router.
- In the router portal, click on “Upgrade”.
- If an upgrade exists, click “Download”, then “Install”.
- Click on “More Settings” > “Network Mode” > “Access Point” > “Apply”.
- Reboot the router, reconnect, test login, and ensure your VPN is active.

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 “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 box 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. Next, let’s focus on the true intention of a portable router.

Assume you are at a hotel and need to access the public Wi-Fi. When you connect your laptop or mobile device, your VPN must be disabled in order to gain authorization through the hotel’s login portal. Once you have internet connectivity, your device will begin to send numerous packets of data exposing your true IP address from the hotel. This traffic will also occur through the hotel’s hostile network.

Personally, I never connect any laptops or personal mobile devices directly through the hotel’s Wi-Fi. Instead, I connect my travel router to the hotel network, and then connect all of my devices through the travel router. This allows me to possess unlimited devices on the network and all of them will be protected at all times by a single VPN connection. The following steps were conducted using a router before and during travel, but could be replicated on practically any portable router using OpenWRT.

Before Travel:

- Power on the device.
- Reset the device by holding the reset button for ten seconds and allowing reboot.
- Connect a computer or mobile device to the router via Wi-Fi.
- Navigate to 192.168.8.1 within your browser.
- Provide a new secure password.
- Under “Wireless” > “2.4G WiFi”, click “Modify”.
- Rename this SSID to something more private.
- Change the security password to something more secure.
- Click “Apply”.
- Repeat the process to rename and secure the “5G WiFi” option.
- Connect your computer’s Wi-Fi to either new SSID of the router.
- In the router portal, click on “Upgrade” > “Download” > “Install”.
- Navigate to <https://docs.gl-inet.com/en/3/app/openvpn/>.
- Apply the appropriate VPN settings for your provider to the router.
- In the router portal, navigate to “VPN” then “VPN Policies”.

- Click the “Enable VPN Policy” toggle and enable the remaining two toggles.
- In the router portal, navigate to “VPN” then “Internet Kill Switch”.
- Enable the toggle option.
- Connect an ethernet cable from an internet connection to the WAN port.
- Test internet and VPN connectivity through your browser.

During Travel at Hotels with Ethernet Connections (Preferred):

- Connect a computer or mobile device to the router via ethernet or Wi-Fi.
- Connect hotel ethernet to the WAN port of router.
- Attempt connection to internet through a web browser.
- If presented a hotel login page, proceed through the process.
- Test internet and VPN connectivity through your browser.

If your devices have VPN-protected Wi-Fi internet connectivity through the router, you are done. The portable router is providing the VPN service to anything connected. The hotel only sees one device (the router) and all data is traveling securely through the VPN. The ethernet connection is typically more stable than Wi-Fi, and I leave the device on for the duration of my stay. Unfortunately, hotel rooms with dedicated ethernet access are becoming rare. If your lodging only provides Wi-Fi, you can still make this strategy work for you.

During Travel at Hotels with Wi-Fi Connections:

- Connect a computer or mobile device to the router via ethernet or Wi-Fi.
- Navigate to 192.168.8.1 within your browser and log in to the portal.
- Navigate to “Internet” and click “Scan” under “Repeater”.
- Under “SSID” select the hotel’s Wi-Fi network.
- If required, enter the password for the network.
- Click “Join”.
- Attempt connection to internet through a web browser.
- If presented a hotel login page, proceed through the process.
- Test internet and VPN connectivity through a browser.

If your devices have Wi-Fi internet connectivity through the router, you are done. I highly recommend leaving the router connected at all times in order to experience as few “dropouts” as possible. With both the ethernet and Wi-Fi options, you may be required to log in to the hotel portal daily during your stay.

Hotel Travel Router Troubleshooting

Since the router is trying to force usage of a VPN, the hotel's network may initially block the connection attempt. Many hotels demand that you first sign in to their own portal to verify that you are an active customer. The portal may refuse internet access to the router until this connection is authorized, which also prevents the VPN connection. Without the VPN connection, the router blocks all internet traffic. This can create a loop of failed requests. During a typical authorization process, the MAC address of a device is whitelisted in the hotel's network for the duration of your stay, and internet access is granted whenever requested. Since the router's MAC address is not authorized, we must "fake" it. During at least 50% of my hotel stays, the previous connection methods fail.

The following steps register a device with the hotel's network and clone that device's MAC address to the router. I usually use my travel "burner" Android device for this process (which possesses the surveillance app Haven as explained later), as I do not like to connect personal devices to hotel networks under any circumstance. I later explain how to create an Android mobile device which never sends data to Google.

- Connect to hotel Wi-Fi directly from a secondary (non-personal) mobile device.
- Authorize the connection through the hotel's Wi-Fi portal.
- Disconnect from hotel Wi-Fi and connect to the travel router via Wi-Fi.
- Open the router portal (192.168.8.1) from a browser and log in.
- Navigate to "More Settings" then "MAC Clone".
- Identify the "Client" MAC address which represents your connected mobile device.
- Under "Your Router", select the MAC address of the mobile device.
- Click "Apply" and test internet and VPN connectivity through a browser.

Let's pause a moment and digest these actions. The hotel's network is blocking the hardware MAC address of the router because it has not been registered. The hotel's network has allowed the MAC address of the mobile device since it was registered. Since we cloned the MAC address of the mobile device to the router, the connection from the router to the hotel should be allowed. If required, you may need to repeat this process every 24 hours.

Some may read the previous section and question my trust of a third party (Slate/Beryl) 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/Beryl is sufficient.

Optional: Embedded pfSense Wi-Fi

Protectli sells an optional Wi-Fi kit which is installed within the device before shipment. It presents an all-in-one firewall and Wi-Fi solution. However, the speeds are typically quite slow. The following steps configure pfSense if you possess an internal Wi-Fi device.

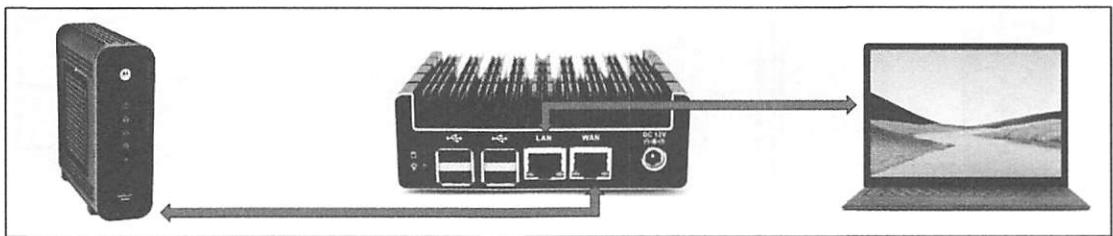
- Within pfSense, navigate to “Interfaces” > “Assignments” > “Wireless”.
- Click the “Add” button and make the following modifications:
 - Mode: Access Point
 - Description: wifi
- Click “Save” and then click “Interface Assignments”.
- Click the “Add” button to add the “wifi” device and click “Save”.
- Click the new “OPT” option at the bottom and make the following modifications:
 - Enable Interface: Selected (checked)
 - Description: wifi
 - IPv4 Configuration Type: Static IPv4
 - IPv4 Address: 192.168.3.1
 - /: 24
 - Channel: 1
 - SSID: pfsense
 - WPA: Enable WPA
 - WPA Pre-shared key: desired Wi-Fi password
- “Save”, “Apply Changes”, then navigate to “Firewall” > “NAT” > “Outbound”.
- Click the first “Add” button and make the following modifications:
 - Interface: OVPNC
 - Address Family: IPv4
 - Source: Network: 192.168.3.0
- Click “Save”, “Apply Changes”, then navigate to “Services” > “DHCP Server”.
- Click “wifi” and make the following modifications:
 - Enable DHCP: Selected (checked)
 - Range: “From: 192.168.3.100 To: 192.168.3.150”
- Click “Save” and navigate to “Firewall” > “Rules” > “wifi”.
- Click the first “Add” button and change the “Protocol” to “any”.
- Click “Display Advanced” and choose a Gateway of “OVPNC”.
- Click “Save”, “Apply Changes”, and reboot the firewall.

During my tests of this configuration, my internet speeds were capped at under 10Mbps. When connected through the Slate wireless router, my speed was 100Mbps. If you possess a slow internet connection and want a simple solution, this may work for you. I do not rely on this strategy due to the low speeds, and I have no clients with this setup.

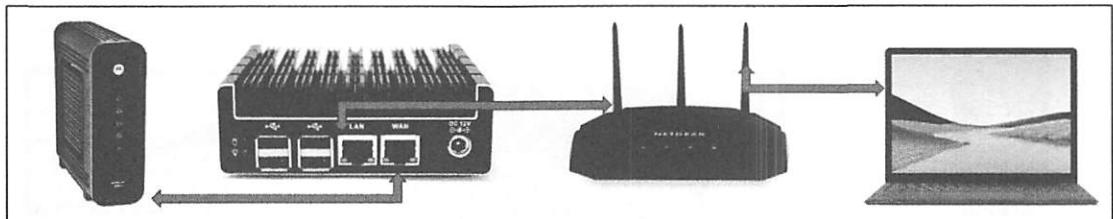
Firewall Summary

This is a heavy chapter. Let's break it down into six 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 after each summary. The modem on the left of each image represents the incoming internet connection provided by your ISP.

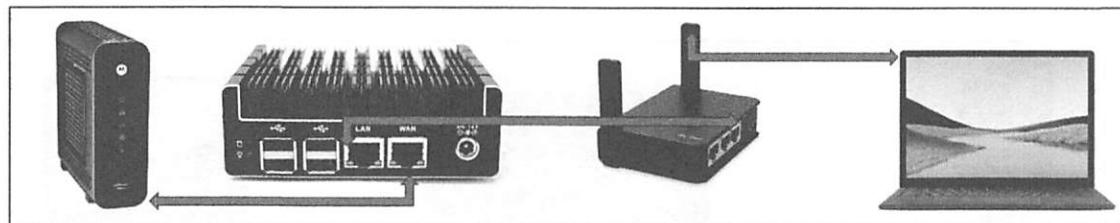
Internet Connection > pfSense Firewall > Wired Devices: This solution provides no Wi-Fi, and should only be considered by those with extreme privacy needs. Your firewall protects all of your internet traffic and you can only connect devices via ethernet wired connections. You will need at least two ports 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.



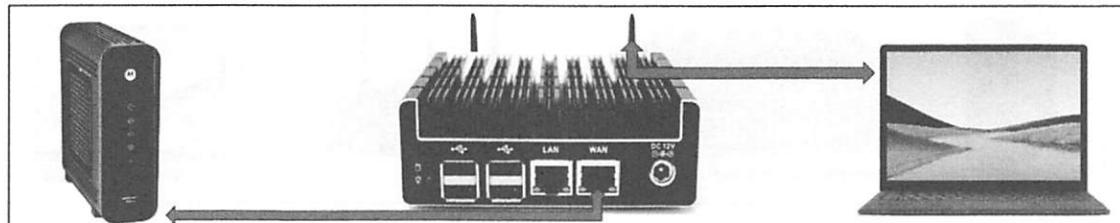
Internet Connection > pfSense Firewall > Open-source wireless router > All devices: This is more realistic for those with other people in the household, and this is the most common execution of this chapter for my clients. The firewall protects all of the traffic in the home with a constant VPN. The open-source wireless router has no proprietary software and all devices connect directly through it. It has a strong range and can support numerous devices. You will be responsible for identifying the appropriate tutorials for installing open-source software such as OpenWRT or DD-WRT in order to replace the stock manufacturer's invasive configuration.



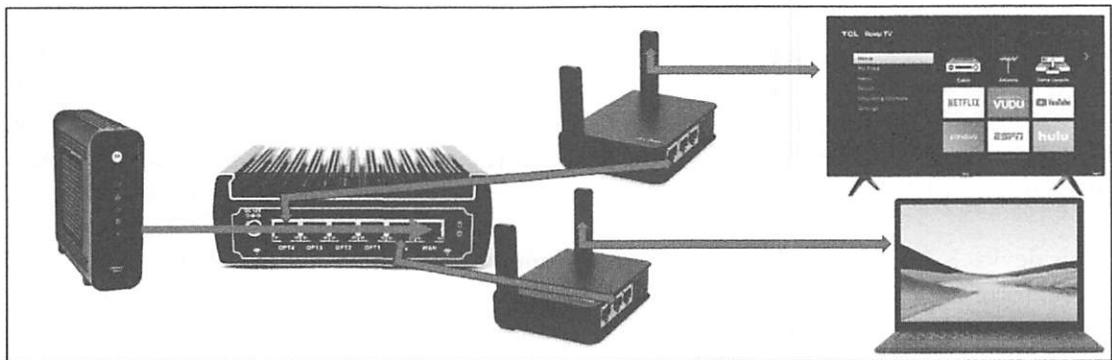
Internet Connection > pfSense Firewall > Portable wireless router > All devices: This is very similar to the previous option, but removes some of the headaches of configuring and maintaining an open-source router. It is the most common scenario for my clients who need a firewall with a static VPN and Wi-Fi which needs minimal configuration. Routers such as the Slate and Beryl previously mentioned are easier to configure and update. They are ready to use right out of the box. Remember that these devices have a shorter range than traditional home Wi-Fi routers and are not suitable for extremely large homes. However, I have installed these within three-story homes without much issue. One benefit of a less-powerful wireless router is that it cannot broadcast signal too far outside the home. Recently, I installed a Slate within a client's home. I could not see the network from the road, but I received a strong signal everywhere within the interior of the home. This is likely an unintended feature, but it gives me more control of my signal.



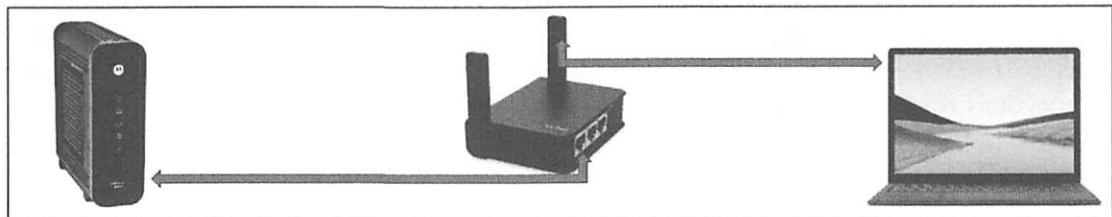
Internet Connection > pfSense Firewall > Internal Wi-Fi > All devices: This option provides a complete network solution within one box. However, the speeds may be slow. All of the Wi-Fi connections are routed through pfSense without the need for an external Wi-Fi access point. I only recommend this for slower internet connections which only require a handful of connected devices. I have also found the range to be less than that of a traditional access point. If your home has a high-speed internet connection which is shared with multiple devices, this is not for you. If you heavily stream high-definition video from various online providers, you and your family will not be happy with this setup. However, this configuration could be used as a standalone travel router. It would provide a stable (yet slow) pfSense firewall with wireless static VPN protection while extending your stay at a hotel.



Internet Connection > pfSense Firewall > “Netflix” 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 a specific 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.



Internet Connection > Portable Router with VPN > All devices: This option relies on the VPN connection as provided within the portable router, such as the Slate or Beryl. This is not nearly as secure or stable as a pfSense firewall, but would provide your entire home the benefits of a network VPN. Ultimately, this should only be chosen due to financial constraints or temporary needs. This is the most common scenario I present while transitioning clients to extended-stay lodging. You may notice your high-speed internet connection slow down when multiple devices attempt to connect simultaneously.



Finally, a departing note. I firmly believe that every “private” home should have a pfSense firewall in between the internet connection and any devices including a wireless router. The choice of wireless access point (router) is not as important when you have a firewall in place, but I encourage open-source options versus standard stock firmware. **Your internet connection may be the most vulnerable and revealing service you ever use. Protect it at all costs.** As a final reminder, all pfSense configuration scripts can be downloaded from my website at inteltechniques.com/firewall.

VPN Wi-Fi Routers

Valid criticism from the previous edition was that I did not include alternative options which were easier to implement but also offered VPN protection throughout an entire home network. While pfSense is more robust and stable, I have tested numerous Wi-Fi routers which possess embedded VPN abilities without the need for additional hardware. Of those tested, I found the **Invizbox 2** devices to perform the best.

This small hockey puck-shaped device connects directly to your home internet connection, such as a cable modem, and shares that connection via Wi-Fi. You provide your VPN credentials during the initial configuration and the device takes care of the rest. The device provides a Wi-Fi network throughout the home and all connected devices route internet traffic through the VPN by default. Sounds easy right? Well, it is, but there are some caveats.

This device is low-powered with less robust resources. This does not impact the ability for it to perform basic VPN or Wi-Fi tasks, but speed may be an issue. If you have gigabit internet coming into your home with twelve devices connected at all times, you will experience an obvious bottleneck with internet speeds. You may see between 30 and 65 Mbps under normal usage. If you have home internet speeds less than 50 Mbps, this may not matter.

Also, you must order a device specifically configured for your VPN provider. This makes installation very easy, but restricts you if you change providers. For most casual users, I believe there is more benefit with this plan than risk. I tested a unit configured for ProtonVPN and experienced no issues. That specific device is located at the following address.

<https://www.invizbox.com/invizbox-2-protonvpn/?l=53>.

In 2021, I issued three of these devices to clients who did not want to fuss with pfSense. They have performed well and served a valuable purpose. Personally, I rely on pfSense for my own home, but I respect some scenarios where a simpler device is warranted.

CHAPTER FIVE

GHOST 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. 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. In 2018, 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 shipping store that provides 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. If you obtain a UPS box, I highly recommend adding the name of a generic LLC to the list of potential recipients. LLCs will be explained later. This will give you an option to have packages delivered to your UPS box in the name of the LLC, or variation of it.

In 2018, I 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 does not possess a home address, and the utility bill displays a former address which will no longer be accurate after a new home is purchased. In every scenario, the address provided was not local to the area. I received no resistance from the staff, and walked out with a new box and key that day.

In 2020, I began 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.

Prior to writing this update, I 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.

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 a UPS box 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.

USPS PO Boxes, UPS boxes, and independent mail receivers 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 big brother.

If you try to open a new bank account and provide a PO Box or CMRA box, you will likely be denied. If you try to use the UPS box on your driver's license, expect failure. Practically every CMRA address has been identified within a database that is used by most financial, government, and related institutions. The moment you place a CMRA address within a credit card application, it is flagged for review. Therefore, a simple PO Box or UPS box is not sufficient for all of our needs. We need a true ghost address that appears like a residential location; allows us to receive mail sent to that address; and never requires us to physically be present at the location. We need a PMB.

A Personal Mail Box (PMB) is much more than a simple PO Box address. It provides you a true residential 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 every client. It is also a vital step toward advanced privacy techniques such as obtaining proper vehicle registrations, driver's licenses, passports, and other identification documents. All of this will be explained in upcoming chapters.

Most states have companies which provide PMB services, but I currently recommend South Dakota for most clients. I had previously considered Texas and Florida as candidates for PMBs, but I no longer endorse these options (unless you will be a physical resident of either state as explained later). Obtaining a PMB is a small part of a larger privacy strategy which is presented throughout the next several chapters, and I have encountered an increasing number of complications with Texas and Florida. However, these states may be considered when we approach nomad residency in the next chapter. For now, I will focus on the only state where I have continued success.

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 chapter 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 exclusively on a service called **Americas Mailbox** (americasmmailbox.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 americasmmailbox.com. At the time of this writing, this form was at the following address.

https://americasmmailbox.com/source/Mail_Service_Agreement_1-3-21.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 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 and driver's license number 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 “home” address. Providing a credit card for payment is acceptable. Again, this is our ghost address. We don't 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 2 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 and maiden names. You should also include the names of at least one trust. Later, I will explain how to use trusts as a layer of privacy within ownership of assets. If you have no trusts listed, mail sent to those trusts might be returned. In my experience, if you have at least one 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.

Boxes 7a through 7e requires a current home address. This can be any mailing address that you currently possess, and I have never witnessed any verification process. Since I assume that you will be moving in the near future in order to obtain true privacy, this can be your current home address or PO Box.

The process through Americas Mailbox requires you to submit a copy of at least one government photo ID. 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 as the following.

514 Americas Way, PMB 143
Box Elder, SD 57719

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 that you reside in a new state. At this point, you are not a resident of South Dakota, you simply possess a mail forwarding service. 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. 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 PMB. Please note this cannot be reversed, so consider your options carefully.

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

ghost 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.

From this point forward, you should give out your new PMB address in situations when you would have otherwise given a PO Box or home address. Exceptions to this include your current driver's license, vehicle registration, and insurance. We are not there yet, but this will be explained later. 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.

In 2017, a client 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 (as discussed later). 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 also have a PMB that collects important mail in your real name and forwards to your UPS box. This can be used for situations that typically block CMRA services, such as banks and credit cards. 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 have 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.

There may be scenarios where a South Dakota PMB is not optimal. If you physically reside in Texas or Florida, it may make more sense to choose a provider in these states. Many clients possess PMB service through a company called **Escapees** (escapees.com). In the previous edition, this was my recommended service. However, I witnessed severe price increases from 2020 to 2021 and demands to join their "RV Club" with further additional fees. This has encouraged me to rely on America's Mailbox for most clients. However, Escapees has other benefits.

Escapees has a presence in Florida, South Dakota, and Texas. This allows you to possess a unique PMB address in each state through one individual account. There are additional fees to forward mail from Florida and South Dakota to a primary PMB in Texas, but this may be justified for extreme scenarios. I have a few clients who have configured PMBs in all three states, but they rarely take advantage of this option. It is overkill for most, and may double your mail forwarding budget. If you plan to execute the nomad residency option presented in the next chapter, these addresses could be vital. I explain more about this soon.

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.

CHAPTER SIX

NOMAD RESIDENCY

I originally hesitated placing this chapter so early in the book. It is extreme to say the least. However, the strategies defined in this chapter 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 stick with the book, as many techniques discussed later do not require you to become a “nomad”.

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 in South Dakota, 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 South Dakota driver’s license or state identification will not suffice. If you are in a similar situation, don’t worry. There are many more privacy strategies in the coming chapters. I want to start here because it is by far the most powerful option.

A previous chapter 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 won't always be easy. However, the final outcome will provide a lifetime of privacy.

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 five years trying to identify the best methods of accomplishing this, and I believe I have perfected the execution.

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 he or she 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 chapter 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 details of our options in the following pages.

South Dakota

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.

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.

Concealed Carry Permits: South Dakota's resident permit is honored by 30 other states and is valid for four years. You must be a minimum of 18 years of age and the cost is \$10. A temporary permit is issued within five days of the date of application. Within seven days of the issuance of the temporary permit the sheriff will submit the application to the Secretary of State who issues the official permit. If you are a PMB holder rather than a permanent resident in South Dakota, you must spend at least 30 days in the state before applying for a concealed carry permit. Under the South Dakota Sunshine Law concealed carry permit information is not considered public information. Many people for whom concealed carry is an important factor have decided against using South Dakota. Because South Dakota issues permits to persons 18 years of age and older, their permit is not recognized by many states. Furthermore, many full-time nomads have no desire to spend thirty consecutive days in the state in order to meet the letter of the residency requirement before submitting their concealed carry application. I present more details about this in Chapter Fifteen.

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 <https://dps.sd.gov/application/files/2815/1085/4078/ResidencyAffidavit.pdf>.

The following page 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.

**RESIDENCY AFFIDAVIT
FOR SOUTH DAKOTA RESIDENTS WHO TRAVEL
AND DO NOT HAVE A RESIDENCE IN ANOTHER STATE**

The purpose of the following questions is to determine if you meet the qualifications for an exception of the proof of residency requirements for obtaining a South Dakota Driver License or non-driver ID card.

This form must be signed by a notary of the public or a South Dakota driver license examiner.

[This can be notarized at the DMV.]

1. Is South Dakota your state of residence? _____ Yes _____ No

[You must select Yes in order to qualify. Since you possess a PMB, that is the technical requirement to declare residency, along with surrendering your previous license.]

2. Is South Dakota the state you intend to return to after being absent? _____ Yes
_____ No

[Again, you must select Yes to qualify. This assumes you will be traveling, will not be physically present within the state, but will return at some point.]

This form must be accompanied by a valid one-night stay receipt (no more than one year old) from a local RV Park, Campground, or Motel 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 if selected.

[In my experience, your chances of being called for jury duty are minimal. If you do get the call, contacting the court and explaining that you do not physically live in South Dakota will dismiss your obligation.]

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 is a major accomplishment. You now have a new license in a state which you do not live in 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. Don't 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 chapter, 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. Before we move on to Texas, there are a few more caveats that I have experienced.

- 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.

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 won’t 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 the previous chapter, 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 previous edition, 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 (americasmmailbox.com) and Escapees (escapees.com). Escapees can help you navigate Florida and Texas residency requirements. 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 2021, and things could be different by the time you read this. As of now, health insurance is technically still required for all 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 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”.

Summary

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 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.

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 final situation a client faced in 2018.

This person executed complete nomad residency through Texas. He went through the steps you read in this chapter. 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.

International Considerations: This chapter 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 chapter. 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.

CHAPTER SEVEN

LEGAL INFRASTRUCTURE

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 it private. This is a holding device 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 chapter 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 chapter 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 chapter 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 chapter 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 can't 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.

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. Then, 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 pages outline a typical living trust template, with an explanation of each section within brackets ([]) and ([]).

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 section identifies you as the grantor and trustee of this living trust. This gives you all of 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 who you are confident will honor the rules of the 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 the remaining people alive receive equal shares of the trust if an alternative 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. These allow the trustee to legally execute various requirements of the trust.]

(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 the page including your signature to be kept on file.]

(New page)

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.

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 that place their home into a living trust have no concern 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 chapter.]

(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]

(New page)

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 these two 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 chapter, I will explain the entire process of purchasing a home with a trust. This action will completely hide the owner (you) from any public records associated with the home. We are not ready for that yet, but this familiarization with trusts will aid during that chapter.

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 chapter, 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.

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 his or her 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 chapters.

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 chapters 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 he or she 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. This person is now the weakest link. A social engineering attack on him or her could reveal something you have spent countless hours trying to hide. Please choose wisely.

Limited Liability Companies (LLCs)

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 section will first explain the power of an “invisible” LLC, then the practical usage, and finally the details of establishing this entity.

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 states to collect the names and identifiers of the beneficial owners of LLCs and share those details with the federal government. 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.

Once the law is applicable, each state will be required to identify the name, physical address, date of birth, and driver's license or other identification number of all beneficial owners of an 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.

Compliance from states is not required until January 2022 for new LLCs, and existing LLCs must provide these details before January 2024. In other words, by the time you read this, creating a new LLC will likely demand your personal information regardless of state chosen.

There are already loopholes being 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 may apply. There are a number of entities 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 create 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 MIGHT not be forced to provide beneficiary details. Please note that I am writing this chapter in mid 2021 before the final regulations have been established.

I anticipate the demand to disclose true LLC ownership details by 2022. 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. 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.

Over the next year, you and I will watch these laws take shape together. I will be monitoring closely and disclosing any new discoveries on my weekly podcast. My biggest concern is that individual states will be responsible for the collection and reporting of this information. I expect unintentional data leaks will cause online exposure through misconfigured servers. I suspect some states will not protect the data appropriately. This may be the best time to create a few “shelf” LLCs for future use.

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 a better option. 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 the best choice.

First, you must find a company that 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 to \$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 of 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. However, I prefer to only use a PMB for things that are heavily associated with your true name. If you have a local PO Box that you use to receive your mail from the PMB, that is a much better option. Your email address can be a ProtonMail account created just for this purpose, and your telephone number can be a MySudo or other VOIP number. Payment can be made using a prepaid gift card or a Privacy.com account (discussed later).

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 the Articles of Organization, which can be found at the following website.

<https://www.sos.state.nm.us/uploads/files/Corporations/dllc.pdf>

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 chapter. The New Mexico Secretary of State website contains more details at https://www.sos.state.nm.us/Business_Services/NM_Domestic_LLC.aspx.

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 December 31, 2120.

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

Bureau Chief

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 chapter.

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 OF YOUR AGENT]
[ADDRESS]**

[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]

Percent: 100%

Date

[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.]

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.]

_____ 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 chapter, 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.

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 will expect to see a claim of this on your yearly 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 be required.

Limited Liability Companies (LLCs) - South Dakota - Nomads

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 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. America’s 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” option.
- Ignore the “Additional Articles” option.
- Ignore the “Recipient” option.
- 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 (explained later), 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 nomad 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. He or she demanded to know your true identity, but withheld it from public view. In this scenario, the agent at your PMB plays this role. He or she 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 still form your own Operating Agreement as outlined previously. 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.

Typical Client Configuration

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, anyone who commits to a full privacy reboot typically receives both a trust and an LLC. The following is usually provided to every client, after a ghost address (PMB) has been established, regardless of nomad residency.

- A trust in a generic name with the client as the trustee
- A Certification of Trust with the client as the trustee
- A trust bank account with the client as trustee
- Checks in the name of only the trust (no personal name or address)
- An Appointment of New Trustee form which assigns a new trustee when needed
- An Appointment of New Trustee form which reverses the trustee back to the client
- An account at America's Mailbox with Registered Agent services
- A South Dakota LLC addressed to the PMB provider and created by a nominee
- An EIN for the LLC from the IRS
- A bank account associated with the LLC
- Checks in the name of only the LLC (no personal name or address)

My clients can then use the trust for home purchases and the LLC for vehicle registration, as explained later in the book. Both the trust and the LLC can be used for all utility payments 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.

Summary

This is an overwhelming chapter. It is very technical, but hopefully provides some insight into the basic foundations of trusts and LLCs. In the next chapter, we can 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 these “behind the scenes” documents is vital in order to execute the strategies in future chapters.

You may have noticed I do not offer digital downloads of these templates. This is very deliberate. I encourage people to completely understand the documents they create. Signing a digital template is easier, but more reckless. I encourage people to always create their own documents and only include details they understand completely. 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 absolute guidance for your own strategies.

International Considerations: 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 sole traders), various types of partnerships, and numerous levels of “limited” companies or organizations. Trusts are widely used internationally, but the documents must conform to the laws created for the specific style of trust. I encourage you to research all options available within your country of residence. Once you find a suitable infrastructure, locate any online templates which should help you understand your own legal document options.

CHAPTER EIGHT

VEHICLES

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. 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 he 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.

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 within this chapter. I present several scenarios which vary in protection from the least to most private.

Current Vehicle Re-Titling to a Trust

First, let's consider a scenario where you are NOT a nomad as defined previously. You possess a vehicle, without a lien, registered in your real name in the state which you physically reside. This chapter will only focus on vehicles without liens. While you can re-title a vehicle with a lien, you are at the mercy of the bank holding the loan. Many financial institutions refuse this, because it is a small asset compared to something larger such as a house. If you push the issue enough, they will likely allow the transfer, but they will often insist that your name appears on the title as the trustee of the trust. This eliminates the privacy benefits of this technique. Therefore, I will assume that you will be re-titling vehicles that are paid in full.

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 sections 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 discussed previously. 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.

Current Vehicle Re-Titling to a Trust (Nomad)

Next, consider a scenario where you plan to become a legal nomad resident of South Dakota. This could also apply to Texas or other nomad-friendly states, but the documentation here is specific to South Dakota. Another advantage of South Dakota is the ability to title a vehicle before obtaining official nomad residency. This allows you test the waters a bit before diving in completely. The final vehicle registration can also be used to justify your connection to the state, which can make the driver's license acquisition easier.

After the PMB is in place and tested, I prefer to immediately transfer any vehicles to the new state of future or current domicile. If you are not a resident of South Dakota yet, but possess a valid physical address within the state (PMB), you can register your vehicles right away. First, gather your title and bill of sale from the dealership or individual for your vehicle. The title will be surrendered to the state and the bill of sale will hopefully waive any taxes owed.

Vehicle registration is an important step toward the transition to a new state, as well as a great verification tool that may be needed to show association as a resident. The order of events while establishing residency is crucial. If becoming a nomad in South Dakota, I recommend registering your vehicles BEFORE claiming residency. One issue I previously faced with Texas is that you must register your vehicles at the time of claiming residency at the DMV. This was not my only reason for moving away from nomad registration in Texas, but issues with the DMV have encouraged me to focus solely on South Dakota.

You will need the following four forms from the South Dakota Department of Revenue, all of which can be found online on their website at <https://dor.sd.gov>. Please note that the state is in the process of switching to a new website vendor, so you may need to search for these forms. 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.

- Affidavit Claiming Lack of Residence Post Office Address (some counties are no longer requiring this form)
- Application for Motor Vehicle Title & Registration
- Applicant's Tax Payment Verification
- South Dakota Exemptions

The nomad affidavit is likely the most foreign document to most clients, and I have included a verbatim copy on the following page. This may require some explanation, which follows. This document is only required if you have not established domicile in the state. I typically register a vehicle before claiming nomad residency, but this is optional.

AFFIDAVIT CLAIMING LACK OF RESIDENCE POST OFFICE ADDRESS

I, _____, in conjunction with my South Dakota Application for Title and Registration, do hereby declare and affirm that the following facts are true:

1. I do not have a South Dakota Driver's License; and
2. I do not maintain a "residence post office address" in South Dakota or any other United States jurisdiction; and
3. Because I do not maintain a "residence post office address" in South Dakota or any other United States jurisdiction, the address I have provided with my South Dakota Application for

(Title and Registration is strictly for mail-forwarding purposes)

Signature of Affiant

Date

Printed Name of Affiant

Notary Public or County Treasurer

STATE OF SOUTH DAKOTA; COUNTY OF _____ Subscribed and Sworn to
before me this ___ day of ____, 20__.

Date Commission Expires

This document is basically a statement of intent. It has three requirements, which I will explain individually. The first is fairly obvious, as you do not possess a South Dakota license (yet). If you already have one, this document is unnecessary. The second requirement is where we must dissect the terminology. Legally speaking, a “residence post office address” is the place where a person actually physically resides. If you are on the move and do not possess a home in South Dakota, this applies to you.

The statement of “the address I have provided with my South Dakota Application for Title and Registration is strictly for mail-forwarding purposes” provides a bit of legal coverage. It clearly claims that you do not reside at the address provided (PMB), and that it is only used for mail collection. You must complete this affidavit and have it notarized locally.

Next is the application for your new title and registration. This 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, which is displayed in a couple of pages.

Section I: This will likely be the first option of Transfer-New-Out-of-State. This notifies the state that you are bringing your title from your previous state into theirs. The optional Brand section is likely inapplicable.

Section II: This should be blank, as you do not have a title yet.

Section III: This is the exact information which will appear on your title and registration. This must be precise. You only need to complete one line in the first section.

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 specific length of a trust title will be explained later. This may be a trust where you are the trustee and grantor, as explained previously.

Type of Ownership: Trust

Customer Type: Trust

Identification #: This should be your SSN. Before you grimace at this, let me explain. This scenario is the second option discussed in this chapter. As mentioned previously, each option adds additional privacy protection. 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. You will need to send a copy of your SSN card or a tax statement, such as a 1099, as proof of SSN, along with this form. 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.

Owner/Lessor/Trust Mailing Address: This should be your PMB address.

Owner/Lessor/Trust Physical Address: This should be your PMB address.

Lessee/Trustee Mailing Address: This should be your PMB address.

Lessee/Trustee Physical Address: This should be your PMB address.

Section IV: Enter the VIN, Make, Model, Body Type, and all other details exactly as they appear on the current title. The odometer reading should be accurate as of the date of completion. The Dealer Price and Trade-in areas can state “Not Applicable”.

Section V: Check the Tax-Exempt box and enter “18” or “99” as the code if you have already paid sales tax on the vehicle through another state. These codes will be explained later. In this section after “3”, enter the date the vehicle was purchased from your original bill of sale. Provide the additional sales price and tax details as obtained from your bill of sale or original title application. Assuming you originally paid at least 4% sales tax at the time of purchase, or when registering within your original state, you will not owe any taxes.

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.

I strongly encourage you to inspect the final page at the end of this form. There are many scenarios where a used vehicle is automatically tax-exempt, such as being at least 11 years of age and sold for less than \$2,500. Before submitting this form, be sure you understand each section. There are many support documents on the state website.

Section VI: If you do not have a lien on the vehicle, this can be blank.

Section VII: If you do not have a lien on the vehicle, this can be blank.

After you have completed all of the forms and gathered your certification of trust, copy of your SSN card (or tax statement), 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 in this chapter, I explained that a lengthy trust name, such as The Motor Vehicle #728495735423001118720438-A Trust, could be valuable for privacy protection. In this scenario, you have provided your real name and SSN 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 SSN card. You also provided your Certification of Trust identifying you as the trustee. Your name is not on the application, but it is on the card and this document. 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.

Date:**State of South Dakota Application for Motor Vehicle Title & Registration**

I. This application is for (Check one only)		Brand (Check if Applicable)		II. South Dakota Title Number				
Transfer - New - Out-of-State <input type="checkbox"/>		Manufacturer Buy Back <input type="checkbox"/> Rebuilt <input type="checkbox"/> Junking Certificate <input type="checkbox"/>						
Interstate <input type="checkbox"/> Operation by Law <input type="checkbox"/>		Manufacturer Buy Back - Rebuilt <input type="checkbox"/>		Salvage Total Loss <input type="checkbox"/>				
Repossession <input type="checkbox"/> Unpaid Repair Bill <input type="checkbox"/>		Manufacturer Buy Back - Salvage <input type="checkbox"/>		Recovered Theft <input type="checkbox"/>		Title County Number		
Abandoned <input type="checkbox"/>		Manufacturer Buy Back - Junking Certificate <input type="checkbox"/>		Parts Only <input type="checkbox"/>				
III. 1-4 Owner/s/Lessor/s/Trust's Name (First, Middle, Last), Description of type of Ownership (and, or, DBA, WROS, Guardianship, lessee, lessor, trustee etc.). Identification Number (SD Dr. Lic., SD ID, Soc. Sec. No. Fed Emp. ID. No.), Description of Customer Type (Individual, Company, Dealer, Government, Trust).								
Owner/Lessor/Trust		Type of Ownership		Customer Type		Identification # (SD DL, SD ID, SSN, FEIN)		
Owner/Lessee/Trustee		Type of Ownership		Customer Type		Identification # (SD DL, SD ID, SSN, FEIN)		
Owner/Lessee/Trustee		Type of Ownership		Customer Type		Identification # (SD DL, SD ID, SSN, FEIN)		
Owner/Lessee/Trustee		Type of Ownership		Customer Type		Identification # (SD DL, SD ID, SSN, FEIN)		
ADDRESS See Special Mailing Address in Section VII	Owner/Lessor/Trust Mailing Address			City		State Zip Code		
	Owner/Lessor/Trust Physical Address (Residence Post Office Address)			City		State Zip Code		
	Lessee/Trustee Mailing Address			City		State Zip Code		
	Lessee/Trustee Physical Address (Residence Post Office Address)			City		State Zip Code		
IV. Primary VIN or Serial Number:								
Make	Model	Body Type	Vehicle Code	Year	Weight/CC	Color	Fuel	Previous State/Brand
Secondary VIN or Serial Number:				Year:	Make:			
Odometer Reading (Complete for vehicles 9 years old or newer):				Units (Check one): Miles <input type="checkbox"/> Kilometers <input type="checkbox"/>				
Odometer Brand (Check one): Actual Mileage <input type="checkbox"/>				Exceeds Odometer's Mechanical Limits <input type="checkbox"/>				
Dealer Price Certification: I hereby certify that the purchase price and trade-in allowance in Item V. of the application is correct and that all accessories and added equipment have been reported.								
Dealer Name and Number		Signature of Dealer or Dealer's Agent				Dealer Sold Permit		
1st Trade-In		2nd Trade-In						
Year	Make	Serial No.	SD Title No.	Year	Make	Serial No.	SD Title No.	
V. Motor Vehicle Purchaser's Certificate (Note: A guide published by the automobile industry will be used to check values)								
1. Tax Exempt (If claiming exemption, list exemption #) _____				Rental Vehicle/SD Sales Tax # _____				
				Non-Profit Donated Vehicle/Corporation # _____				
2. Title Only (If applying for a "Title Only," in signing this application you are attesting that the vehicle will not be used upon the streets and highways of this state or any state. Application must be made within 45 days of purchase date.)				VI. Important: Electronic Lien & Title - A paper title is not issued until lien(s) released or upon request by lienholder for other approved purpose.				
3. Purchase Date				1st Lienholder:				
4. Purchase Price (see Reverse Side) Bill of Sale Not Available Computer NADA'ED				Mailing Address:				
5. Less Trade-In Allowance				City/State/Zip Code:				
6. Difference				2nd Lienholder:				
7. Tax 4% of Line 6, Snowmobile 3%				Mailing Address:				
8. Tax Penalty & Interest				City/State/Zip Code				
9. Credit for Tax Paid to Another State				To add additional lienholders, see section XI on reverse side				
10. Title Fee				VII. Special Mailing Address: (If other than owner/lessor address)				
11. Late Fee (Application made after 30 days)				Name:				
12. Lien Fee				Address:				
13. Balance Due for Title Application				City/State/Zip Code:				

The applicant, under penalties of law and as rightful owner of the vehicle described on this application, declares that the information set forth on this application is true and correct.

PENALTY: Any person failing to pay the full amount of excise tax is subject to a Class 1 misdemeanor.

Signature _____
Date _____

PENALTY: Any person who intentionally falsifies information on this application is guilty of a Class 6 felony.

Signature _____
Date _____

MV-608 (05/12)

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. The following is an example of this form, SD 1731.

South Dakota
Division of Motor Vehicles
Applicant's Tax Payment Verification

This form must accompany South Dakota's application for title to qualify for credit against South Dakota's motor vehicle excise tax for a like or similar tax paid to another state on the purchase of a vehicle. The out-of-state title being surrendered must be in the same name as the applicant. The applicant receives credit for the percentage of tax paid that is equal to or greater than the tax owed to this state.

Name _____

Street _____ City _____ State _____ Zip _____

Amount Paid _____ Tax Type _____ Sales tax was paid to _____

Date of payment

Date of payment _____

This statement is made with the knowledge that it is a Class 5 Felony to make a false statement and that in doing so, I am subject to the penalty of South Dakota law.

Applicant's Signature

Date

The final document is the South Dakota Exemptions form which is only required if your previous title was in your real name and you want the new title to reflect your trust name. This is a powerful step in this process. It is quite easy to transfer the title from one state to another if the owner information remains identical. Since we are changing the name of the owner (from you to your trust), we must request a waiver of vehicle sales tax.

The previous form explained 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. Therefore, this form will request to waive the taxes since you are technically still the owner.

Since you do not possess a title number yet, leave the first field blank. Supply the odometer reading on the vehicle (miles), and place "NONE" in the lien holder field. The tax exemption code, which was also provided within the application, should be "18" or "99". A code of "18" indicates that at "motor vehicle/boat transferred by a trustor to his trustee or from a trustee to a beneficiary of a trust". This summary is not exactly your scenario, but it is the only option on this form acknowledging a trust. Technically, you are a trustor transferring to the TRUST.

A code of "99" is often a catch-all or "other" option which allows the employee to determine the appropriate assignment for the title. I have spoken with numerous employees of the South Dakota Division of Motor Vehicles over several years about these. They have all agreed that either exemption can be appropriate for the purpose of transferring a vehicle from an owner into a trust created by that same owner. Please call them to determine the current recommendation for your scenario.

Include a certification of trust as explained in the previous chapter 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.

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).

SOUTH DAKOTA EXEMPTIONS

This form is to be used when claiming an exemption from the South Dakota excise tax on a South Dakota titled vehicle/boat.

South Dakota Title Number _____

Odometer Reading is _____ which is actual vehicle mileage

1st Lien holder _____

Mailing Address _____

City _____ State _____ Zip _____

_____ Tax Exemption being claimed (indicate number)

BY SIGNING THIS FORM YOU ARE ATTESTING THAT THE EXEMPTION BEING CLAIMED HEREON IS TRUE AND CORRECT. ANY PERSON WHO INTENTIONALLY FALSIFIES INFORMATION ON THIS FORM IS GUILTY OF A CLASS 6 FELONY.

Signature

Date

Let's catch our breath here and summarize a few things. In the first scenario, you own a vehicle in the state you 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 the second scenario, you are leaving your current state and PLAN to become 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, he or she 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 plan on eventually executing full nomad status. 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.

New Vehicle Purchase Through a Trust (Non-Nomad)

Next, assume you are NOT a legal nomad and will be buying a new 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 in 2018.

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 chapter.

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.

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 can't stress enough that your mileage will vary with this. Every state has its own nuances and policies. Each employee at the DMV may have his or her 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, he or she 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.

New Vehicle Purchase Through a Trust (Nomad)

Finally, 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 not difficult. 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 exception is California. If you purchase a car there, you must pay the inflated California 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 (not you). This trustee has the powers to sign on behalf of the trust, but will need to disclose their SSN to the state. This can be very invasive, so make sure you have a trustee willing to participate at this level. 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. The dealer will complete the title application on your behalf and determine the amount owed to South Dakota for taxes and registration. The other documents completed previously are not required because you have established domicile and are not requesting a waiver of taxes. Your trustee will sign the paperwork and you will pay in cash via cashier's check. 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 and your trustee. 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 chapter have already explained the overall process.

New Vehicle Purchase Through 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 many 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 previous instruction 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. However, there is one last option, which has proven to be the most beneficial strategy for my clients over the past year.

New Vehicle Purchase Through an LLC (Nomad)

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 from late 2019. This revisits some of the content already presented in this chapter, 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 be used 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 SSN, 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 person who buys vehicles on behalf of a taxi service. His or her name is 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. 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 a sales person has a potential purchase scheduled, he or she has 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 "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 won’t 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 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 include 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 don’t 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 displayed previously in this chapter, and I used the same form for my nomad client. However, there were a few important differences. The first line in section three 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. Lines 4 through 14, which identifies 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.

Insurance

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. 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.

Loans

All of the scenarios I presented involved a vehicle purchase with cash. If you require a loan, it will complicate things. While many lenders will title a home loan in a trust, most vehicle lenders do not like this. 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.

Choosing a Vehicle

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
Honda Accord
Honda Civic

Toyota Rav4
Toyota Camry
Honda CR-V

Toyota Corolla
Dodge Ram
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.

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 brand 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 or make and model identifiers are not mandatory. There are no laws that demand constant announcement of the type of 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. The next time you are in a parking lot, imagine each car without the emblems placed at the rear. It would be difficult for the common driver to identify each.

As part of this request, ask that the removed emblems and decals be preserved and given to you. When you sell the vehicle, the next buyer may desire these decals be present on the vehicle as a status symbol. They can always be glued back onto the vehicle. If you plan to execute this strategy, I encourage having the dealer remove the signage. They have the proper equipment to do this easily and without damage. Popping these off with a flathead screwdriver in your driveway will likely produce undesired results. Removing vehicle markings can also backfire on you. If you have a very expensive car, such as a Porsche, with no decals, you may stick out more. You may be described as “the Porsche without the decals”. This makes you more unique. I offer this strategy only for the boring vehicles, such as common cars and trucks. For a more exciting approach, you could purchase inaccurate logos from an auto store. Place a Ford logo on the rear of your new Toyota. This is a level of disinformation that will confuse many. While I present this strategy as half-humor and half-intentional, I do not recommend this technique for everyone as it could make your vehicle more unique. I will confess that my truck has absolutely no markings, logos, or dealer advertisement whatsoever.

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).

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.

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 titled “I Want To Remain Anonymous” at <https://goldengate.org/tolls/iwanttoremainanonymous.php>. 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 hunt you down, 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 provides 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.

Private 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 podcast about the issue (Episode 118: How Neighborhood Watch Watches You).

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. He or she 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, he or she has 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). 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, he or she likely has 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 site 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.

Vehicle Privacy

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.

Auto Supply 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	Controller ID Number
Credit Card Information	Trouble Codes
Vehicle Year	Vehicle Diagnostics
Vehicle Make	Store Location
Vehicle Model	Vehicle Parts Purchased
Vehicle Identification Number (VIN)	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 chapter 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 true names to vehicles during any type of service or scans. 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.

Vehicle Tracking

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 your car, remotely start the vehicle, be notified about upcoming