

maintenance, or receive a notification of a collision. In order for this to work, a paid service associates your vehicle with your mobile device. The vehicle possesses an ability to connect to the internet, likely through a cellular modem, and the service allows it to maintain a connection to Nissan. This convenience presents two issues.

First, there is a huge security concern. If your phone is lost or stolen, there is an avenue to breach your vehicle. Even if your device is safely in your possession, car hackers have proven many times that vehicles are prone to unauthorized access. Next, there are several privacy implications. The privacy policy for NissanConnect states very clearly that they can share any data about you and your vehicle with other companies. In 2020, Nissan updated their policy with the following entry, without any consent from users.

“If you are a registered Nissan owner and NissanConnect Services subscriber, this update allows Nissan to share information such as your vehicle’s mileage and vehicle location with third parties.”

If you have already downloaded a mobile application provided by your vehicle manufacturer, registered an account through their service, and associated your vehicle to the account, you should consider wiping your tracks. This should be done in a very specific order.

- Attempt to remove any accounts within the vehicle’s infotainment unit. You might see a profile in the settings menu.
- Conduct a hard reset of the infotainment unit, which should return the configuration to the default which was present during purchase. You may need to find instructions within your vehicle manual or online.
- Disconnect the vehicle battery for at least one minute, which may remove leftover unwanted data.
- Through the app on your mobile device, attempt to remove any association to your vehicle. Afterward, uninstall the app from the device.
- Log in to the account through the designated web page within a web browser. If the vehicle is still present, attempt to remove the association.
- Attempt to delete the entire account within the account settings menu. If this is not allowed, contact the service and demand removal of all data.

You may think this is all overkill. If you do, I present the story of Mathew Marulla, as originally reported at KrebsOnSecurity. Mathew leased a Ford Focus electric vehicle in 2013, but returned the car back to Ford at the end of his lease in 2016. In 2020, he received an email from Ford stating that the clock in his car was set incorrectly. Marulla’s credentials from 2016 still worked on the MyFord website, and he was presented with an online dashboard showing the current location of his old vehicle and its mileage statistics. The dashboard also allowed

him to remotely start the vehicle, as well as lock and unlock its doors. He provided the following statement to Brian Krebs.

“I can track its movements, see where it plugs in,” he said. “Now I know where the current owner likely lives, and if I watch it tomorrow, I can probably figure out where he works. I have not been the owner of this vehicle for four years”.

If you plan to buy a used car, you should check whether it is possible to reset the previous owner’s control and information before purchase. You may also consider demanding that the dealership completes this task. My vehicle tracking rules are quite simple.

- Never purchase a vehicle with an embedded cellular connection. This includes OnStar or any similar competitor. Even when deactivated, the connection still allows remote access and submits data back to the provider.
- Never purchase a vehicle with embedded navigation including real-time traffic information. This indicates an active connection to the manufacturer.
- Never connect a mobile device with internet access to the infotainment unit of the vehicle. This allows data to be sent to the manufacturer.

When playing by these rules, you will encounter minor inconveniences. I received the following complaints from my clients, which include my recommended solutions.

- **Navigation:** Seeing your navigation map on the in-car display is nice. It might also share internet with your vehicle’s reporting system. My only solution to this is to rely on your mobile device’s navigation on the device’s screen. If necessary, mount the device above your dash using a suction mount.
- **Music:** One benefit of connecting a mobile device to the vehicle is the ability to stream music stored on the device or from online streams. Most modern vehicles possess a USB port which accepts flash drives full of MP3 files. My own vehicle allows a 256GB flash drive containing hundreds of albums worth of music. I play the files through the main infotainment dashboard.
- **Podcasts:** Streaming a podcast from your mobile device through your vehicle’s Bluetooth is very convenient, but risky. You could load MP3 audio files of podcasts onto the USB drive mentioned previously, but that can be daunting. Instead, I recommend simply connecting your mobile device to the audio auxiliary (AUX) port. No data is transmitted through this 3.5mm audio input.
- **Hands-Free Calling and Texting:** I understand the desire to connect your phone to the vehicle in order to make calls while driving. Many state laws allow this but have ruled touching the phone as illegal. My only solution here is to avoid calls and texts while driving. I know this is unpopular, but we survived without it for decades.

Insurance Apps

I avoid installation of any applications created by my vehicle insurance provider. While you may receive a slight discount in exchange for activating their app, all benefits to you stop there. The insurance companies have much more to gain from your willingness to share personal data with them. The biggest concern is the potential abuse of location information. Many vehicle insurance applications quietly run in the background at all times. They use your constant location to determine speed of travel and other driving habits. This data can then be used to determine your premiums. It can also be used to identify the location of your home, workplace, lovers, and entertainment. Did you park outside a pub for three hours and then race home? That would be documented forever. A dishonest I.T. employee at the insurance company could gain access to this data, and a court order could demand legal release of all collected details. I will not take this risk.

Summary

I realize this can be overwhelming. I have always resisted providing this level of detail in my books in order to prevent confusion or provide too many options. We do not need to overcomplicate the issue. Overall, there are three vehicle purchase choices which will lead you to the appropriate answers.

- Do you own a vehicle titled in your name? Transfer to a trust, with you as the trustee, within your state of residence or domicile. Ensure that the trustee name is not present on the owner line of the application and that only the trust name is displayed as the owner of the vehicle. If this is not possible in your state, consider the following options.
- Are you buying a new vehicle? Title into a trust with someone else as the trustee within your state of residence or domicile. Ensure that the trustee name is not present on the owner line of the application and that only the trust name is displayed as the owner of the vehicle. If this is not possible in your state, consider the next option.
- Does your state enforce publicly displaying the trustee name on the title and registration? Consider the LLC route. Seek approval from your insurance provider and investigate any state requirements for foreign business registration and taxes. This route may be more expensive, but may be your only option in a few states.

In any scenario, make an effort to exclude any name and home address from the registration. This step will prevent multiple private companies from collecting, recording, sharing, selling, and accidentally leaking your personal information to the masses.

CHAPTER NINE

TEMPORARY HOUSING

I have not booked a hotel room under my true name since 2013. This may sound ridiculous and paranoid, but since you are this far in the book, I accept this risk. In late 2012, I was scheduled to present a keynote at a large conference in Florida. This was a very public event, and the roster of presenters was available on the conference website. I was contacted by a person asking if I would be willing to meet her for dinner the night before my session. She wanted to “pick my brain” about some issues she was having, and knew I would be in town. A quick search of her email address revealed dozens of messages sent to my public email address listed on my website. These messages were very concerning, and included allegations of alien probes, government chips in her head, and an overall theme of mental instability.

I politely declined to meet, citing a late flight and early morning. She responded notifying me that the last flight into the local airport from St. Louis arrived at 6:15 pm and that we would have plenty of time. I again declined, and did not think much more of it. I arrived at my hotel at 7:00 pm, checked in, and walked to my room. A woman was following me, so I took a detour into a stairwell. She followed and sternly stated that she needed to talk with me right away. I returned to the lobby, and we had a very brief conversation. I clearly explained that her actions were inappropriate, and she agreed to leave. I did not sleep well that night.

This may sound like minimal risk and you may think I am the jerk for declining to help her. For a moment, replace the players. Pretend my role is played by a successful woman in the entertainment industry, and the original woman is now a male fan that has sent threatening letters. It may not seem so crazy now. This scenario happens every day. Many of my clients find themselves constantly harassed by people that just want to be closer to them. This includes celebrities, business leaders, and domestic violence victims. You do not need to be famous to have a violent person in your life. Therefore, we must have plans for anonymous housing, even if temporary.

This chapter is a transition in order to prepare you for the ability to purchase your next home anonymously. While you are hunting for the perfect new home, you will need temporary housing. This chapter will define temporary housing as short-term options such as hotels and longer-term solutions such as rental homes. Let’s start with the easier of the two, hotels.

Obtaining a hotel reservation is very difficult without a credit card. Some hotel operators will reserve the room without a guarantee that it will be available. Some will refuse the reservation without a valid card number. Lately, many hotels apply the entire charge for the visit at the moment of the reservation. When you arrive, you must provide the card at the front desk to be swiped. This collects the data about the cardholder and attaches it to the sale. There are two main reasons for using an alias while at hotels.

When you stay at a hotel, there is a lot of information that the business can analyze about you and your stay. The amount you paid, the length of your stay, any amenities you purchased, and the distance you traveled from home will be stored in your profile. This will all be used to target you for future visits. Worse, it will be shared with other hotels in the chain that can benefit from the data. Even far worse, all details are leaked publicly through a data breach, similar to the Marriott breach of 2018.

A more serious concern is for a person's safety. If you are the victim of a stalker or targeted by someone crazy in your life, it is not difficult for them to find out the hotel where you are staying. The easiest way would be to contact every hotel in the area where you will be traveling. The following conversations with a hotel operator will usually divulge your chosen hotel.

"Hello, I made a reservation there a while back and I need to add an additional day to my stay. I may have put the reservation under my wife's name, Mary Smith. If not, it could be under my name, Michael Smith. I'm afraid I do not have the reservation number; can you find the reservation without it? It is for next week."

The operator will either be unable to locate your reservation or confirm that an extra day was added. The first call which receives the confirmation will identify where you are staying. A simpler approach may be the following.

"Can I leave a message for Michael Bazzell? He is staying there now."

The response will either be, "We do not have a guest here under that name", or, "Yes, go ahead and I will leave the message at the front desk for him".

A more high-tech approach could be conducted through the hotel's wireless internet. Many hotels require you to log in to the wireless internet before you use it. This usually requests your last name and room number as verification that you are a valid guest. Some amateur programming can create a script that will attempt to log in with your last name and each room number of the hotel until the attempt is successful. This not only identifies the hotel where you are staying at, but exposes your room number. This can be a huge security concern.

You can use an alias name to create your hotel reservation. Since you are not committing any type of financial fraud, I believe this is legal. You will be providing a legitimate source of payment and will pay all charges in relation to the stay. There are three main attacks for this, as outlined in the following pages. The first requires no identification, but carries a bit of risk.

Many hotel chains offer prepaid reservations and digital check-in. I have had the most luck with Hilton properties. I recently needed to travel domestically to an airport hotel, and then internationally for a few days. I wanted to stay off radar and test a new strategy on which I had been working. I have had the best success with the following routine.

- Create a new rewards account with a large hotel chain, preferably Hilton or Marriott. Use any alias name, and any physical address, such as another hotel. The longer this account can “age”, the better your chances of success.
- While logged in, search the hotel website for a hotel near the desired location. Watch for notifications about “Non-Refundable”. This is actually the desired option.
- Attempt to identify hotels that offer “Digital Keys”. This allows you to use a mobile device to unlock the door to your room, often bypassing the front desk.
- Book your room, pay with a private credit or debit card. Many payment options will be explained later. Use the same alias details connected to your alias rewards account.
- The day before your stay, “pre-check-in” to your reservation and choose a desired room with the hotel’s interactive online reservation system. Most Hilton properties allow this.
- If you selected a hotel with a digital key option, you should be able to unlock the door with your mobile device. This requires the hotel app to be installed, so I maintain an old Android device solely for this purpose. You can connect to the hotel Wi-Fi through this device and unlock the door from the app.

As always, there are caveats for this to work. Generally, the first time you use this feature, the hotel will ask you to check-in with the front desk. They may want to see identification and the credit card used during the registration. The Hilton website makes this clear with the following disclaimer.

“For Digital Keys: Most new digital key users will need to stop at the front desk upon arrival to activate their digital key. Must have iPhone 4s or newer running iOS 8 and higher or an Android phone running version 4.3 or higher with Bluetooth Low Energy enabled phones.”

I have used this technique on numerous occasions. The resistance from the employees at the front desk has varied. In three recent attempts, each with new rewards accounts, I was able to gain entry to my room without displaying any type of identification. All three required me to

check-in with the front desk before my phone could be allowed to unlock my room. In all three, I opened the communication with the following dialogue.

"Hi, I have a room prepaid with digital key check-in, but my app says I have to check with you to enable it. Can you help?"

In each scenario, the hotel employee requested photo identification and the credit card used. My response each time was the following.

"I didn't bring my wallet in with me, and my ride has already left. I assumed since I could use my phone to bypass the front desk you would not need that. In fact, your site says that would be the case. If you would like, I can show you my app, confirmation, and receipt of purchase to justify the stay."

This verbiage has always de-escalated any resistance. You may encounter a difficult employee that stands his or her ground and demands identification. When this happens, I have found a polite request to bring my ID before check-out works. I also always have the Hilton website discussing the ease of digital keys pulled up on my mobile device web browser, which I can display to the hotel employee in my defense. It can currently be found on their website at <https://hiltonhonors3.hilton.com/en/hhonors-mobile-app/digital-key.html>.

I have also tried prepaid options without digital keys, and had no issues at check-in. When I did not have the option for digital keys on the website, my room card was waiting for me at the front desk. Since the rooms were prepaid, I was usually not asked for any ID or credit card. The vital piece for all of this to work is to book rooms which are completely prepaid, non-refundable, with successfully charged fees through your payment method. Once the hotel has received their payment, identification and credit card requirements are more lenient. If you are pushed to provide the physical credit card used during purchase, blame your employer. I have found stating, "My work paid for the room with a corporate credit card. I WISH they trusted me with having a card, but you know how THAT goes". I have yet to be challenged on this.

I will end with a warning. This could fail. You may be denied a room. I find this to be highly unlikely, but it could happen. Also, if you need to cancel a reservation, you will not receive a refund. I only provide this information for those that need it. Domestic violence victims, stalking victims, and those under a temporary spotlight may find this useful. I consider many options when I assist someone with disappearing completely.

In early 2020, I attempted these techniques at an affordable hotel in an urban area. I could sense suspicion from the staff toward every customer. This hotel was in a high-crime area, and the employees seemed on high-alert. I dished out every excuse in the book as to why my client,

a domestic violence victim who fled her tech-savvy abuser, had no government identification in the name matching the registration. They were not budging. I was told that she would not receive a room without ID and a physical credit card in that name. I advised I would make a call and come back in a few minutes. A quick Google search identified the hotel owner's name and Truepeoplesearch.com disclosed his home address and landline telephone number. Out of desperation, I told the clerk, "I just spoke with (owner name) and he asked you to call him at home at (home number) if there were any problems. He is a friend and is helping me relocate an abused woman". I sweated a bit from my ruse until she said, "That's fine, I am not calling him this late". That night, I began questioning this line of work.

The next tactic provides more assurance that you will have a smooth interaction with the front desk, and check in under an alias with no resistance. This requires a credit card in an alias name, which is explained in the upcoming anonymous payments chapter. These are fairly easy to obtain and are completely legal. The difficult part of this plan is identification in the alias name. Many people will not be comfortable with the following methods, but my clients in fear for their lives have no issue.

First, create a new rewards account with a large hotel chain, preferably Hilton or Marriott, as previously mentioned. Use any alias name, and any physical address, such as another hotel. This can be created the day of the booking. Upon arrival at the hotel, hand your alias credit card (explained soon) to the receptionist. You will likely be asked for identification. In my experience, stating that your wallet was stolen and you only have the credit card because you keep it in the car is sufficient if you really "sell" it. Your success will vary widely. I always recommend persistently denying that you have ID if you have nothing with your alias name on it. Possessing your rewards card in your alias name is often enough to pacify the request. Very few hotels will turn down a loyal paying rewards member with a credit card in hand. I find that being polite and understanding always works better than acting agitated.

If this does not work, have a travel partner show identification to meet the requirement. This information will most likely not be added to the reservation, and cannot be queried. In 2017, I was checking into the Mandalay Bay under an alias name before the BlackHat conference, where I was teaching a 2-day privacy crash course. I provided my alias name and credit card, but the card was declined. I had not used that card for many months, and the provider blocked the charge as suspicious. Fortunately, a colleague was with me and stepped in with his credit card and ID to meet the requirement. He was not staying in the room, his details were not attached to my stay, he was not tremendously exposed, but he would get billed if I trashed the room (I did not). This is not the best option, but will suffice if desperate.

I prefer a third option. I possess alias identification at all times. Hear me out before you believe I am breaking the law. I would never condone obtaining a real or fraudulent government identification card in your alias name. Not only is that illegal, but completely unnecessary.

Instead, I create my own “club”, which I am the founder (as my alias name of course). For example, you may be very interested in rock climbing. You could start your own organization titled “The Greater Houston Rock Climbing Gym”. Maybe you have some steps on your back porch that you use to “climb”. Your definition of climbing might be different than others. Now, you may choose to create an identification card for the members of your backyard gym. This could be completed in Microsoft Word and may include a photo of you. Your local print shop will happily print this on a nice paper stock and laminate it for you. The following should work well at the check-in of your hotel.

“I’m sorry, I left my license at the gym, can I show you my gym membership card until I go back to get it?”

I have also found employer identification to satisfy a demand for ID at a hotel. Assume I possess an LLC titled “The Workplace LLC”. I can create an employee identification card containing my photo, alias name, and company logo. I can then place this laminated card into a lanyard around my neck during check-in. The moment I am asked for identification, I do a quick pat-check for a wallet on my back pants pockets and then instinctively grab my lanyard. I pull it toward the employee and allow them to verify that the name matches the credit card. This has never failed me. For added comfort, I add the line “For novelty purposes only, this is not a true ID, and is not to be used for any official identification” on the back (which is never seen unless inspected closely).

There has always been great skepticism about the legality of using an alias. I firmly stand by my views of when it is legal and illegal to use an alias throughout everyday encounters. I offer my opinion.

- **LEGAL:** Non-government identification in an alias name can be legal. There should be absolutely no mention of any government entity. There should be no mention or reference to any real businesses. It should not identify you as an employee of a legitimate company which you do not own.
- **NON-LEGAL:** Any false identification that displays the words city, county, state, government, police, license, driver, court, agent, et cetera is a crime. Any reference to ANY government agency is also illegal. Any resemblance to a real driver’s license will get you arrested.
- Never use an alias when identifying yourself to a government official.
- Never use another person’s SSN or known real name and DOB combination.
- Never attempt to obtain any credit under an alias name.

Overall, I believe it is legal to provide an alias name to a privately-owned hotel. Do you think famous celebrities stay under their real names? I can verify from personal experience they do not. Why shouldn’t you have the same luxury? After the Marriott breach in 2018, people asked

if I was concerned. I was concerned for other people, but not myself. My true name does not exist within it. My stay history and payment methods are all in various alias names that are not associated with me. I anticipate more hotel breaches will happen, and my true details will not be exposed.

If you are still uncomfortable possessing an alias identification card with alias credit card, there are other options. I have had great success using services such as Airbnb for temporary stays. In fact, it can be easier than traditional lodging. I have arranged lodging through this service for myself and clients. I simply needed to create an account in an alias name, provide some standard details such as an alias email address and telephone number, and select the property where I needed to stay. I always try to find a location that appears to be a secondary home of the provider or an apartment detached from the renter's residence. Once you have provided acceptable payment through the service, such as an anonymous payment source that is explained later, the individual provider is happy to hand you the keys. They rarely ask to see any type of identification or proof of credit card. Often, a code to a digital lock is given and you never have any contact with the host. This situation can be much less stressful than convincing a hotel clerk you are someone else.

I have had several clients recently report that services such as Airbnb were becoming stricter toward new accounts. Rental attempts using a new account, prepaid card, and alias names were being rejected because of new fraud prevention strategies. I no longer book directly through Airbnb. Instead, I contact home-owners directly, outside of the application. This is legal to do, but the Airbnb members may be violating policy by conducting business outside of the app. I often use the Airbnb website in order to identify the place where I want to stay. I then conduct a search of the address within various people search websites and identify the owner. Finally, I contact them directly through a publicly listed email address and offer cash for the stay. Some avoid this for liability reasons, but most welcome an opportunity to be paid in cash and avoid the Airbnb fees.

The idea of providing an alias name and anonymous payment method works in most short-term stay situations. Whether a traditional hotel, extended stay alternative, or privately-owned property through an online service, they all simply want to be paid. They also want empty rooms filled in order to meet strict quotas. As long as you ensure that payment is made and that no financial fraud occurs, you should have no issues using an alias. If you need something more long-term, you will need to change your strategy.

In 2020, I began registering most hotel rooms in a business name. This cannot usually be done online, but a call during business hours works well. I explain that I would like to prepay for a block of rooms in the business name and make sure my employees are not charged anything. In this situation, hotel staff are much less scrutinous toward ID and payment options. Your experiences may vary, but this is another tool to possess.

Finally, I offer the safest and least sketchy option for semi-anonymous hotel stays. In 2021, I noticed many clients were concerned with possession of a credit card or identification card in an alias name. I respect this anxiety, and I outline more considerations with alias IDs later in the book. While possession of a non-government laminated alias ID can be made legally, you are always at the mercy of police officers, detectives, and prosecutors if you are believed to be acting in a way that violates any one of thousands of local laws. I am probably more comfortable than most with alias ID usage due to many years working under-cover and possessing multiple legitimate government-issued driver's licenses in various names. Today, I question the level of need for alias ID and credit cards for most of my clients. However, I still need to create temporary lodging reservations without using a true full name. I must balance privacy and security concerns with the ability of the client to execute a strategy comfortably. The following has worked well for short-term stays.

Assume your name is Michael Aaron Bazzell. If you create a hotel reservation in the name of Michael Bazzell, you are quite easy to track. There are few people in the world with that name and a few calls to local hotels should locate you quickly. Instead, consider creating the reservation in the name of Michael Aaron. This is a much more generic name. While your adversary may know your middle name, he or she may not think to begin a hunt for this name. More importantly, this is not a lie. Your name is Michael, Michael Aaron, Michael Aaron Bazzell, and Michael Bazzell. Even better, you already possess an ID with this information. Your driver's license likely displays your full name on a single line, such as "Michael Aaron Bazzell". However, a United States passport and passport card displays this data on two lines, similar to the following.

Surname:

BAZZELL

Given Names:

MICHAEL AARON

When an employee at the hotel asks to see ID, he or she is quickly scanning for the appropriate data, such as "Michael Aaron". When this is seen in the "Given Names" section, the demand is satisfied. On only one occasion, I witnessed a hotel clerk question the full name not matching the reservation. I simply stated "You are correct, Michael Aaron is my given name but the passport division requires a surname to be added to all cards". This is absolutely true and means nothing, but it provided enough explanation to move on with the process. Obtaining a credit card displaying your first and middle names is quite easy, and is explained in Chapter Eleven. I believe this strategy violates no laws. However, it also provides the least amount of protection. If my client has a unique middle name or is running from a physically abusive person, I never consider this tactic. If you simply want a low level of anonymity while you attend a conference, I believe this is a strong consideration.

Reward Programs Concerns

Most enjoy a free stay or a complimentary upgrade at a hotel due to loyalty points. However, these come with serious privacy disadvantages. When you use the same loyalty account for all of your stays, you create a permanent record of your travel. You also generate a pattern of your history which could be used to determine future locations. If you always stay at a specific hotel over winter holidays while you visit family, and I can see your past stays on your account, I can assume where to find you at the end of the year. Theoretically, only hotel employees should be able to access these details, and this may not be a huge threat. Unfortunately, data breaches, rogue employees, and social engineering make this information visible to anyone who desires it. The simple solution is to either possess several loyalty accounts or none at all.

I currently have a loyalty card with both Hilton and Marriott in three different aliases. I switch it up while I travel and book my rooms with the lessons explained previously. However, if I am staying at a property where I will be meeting a high-risk client, I use no loyalty account at all. I use a clean alias with no history. These rewards profiles can assist with smooth check-ins, but come at a price. There is always a trail and you cannot delete your account afterward.

In 2017, I possessed the highest tier of rewards for each major hotel provider. I received frequent room upgrades, free cookies and fruit plates, and more free stays than I could use on personal travel. However, I gave it all up. The perks did not justify continuing the tracking of my whereabouts, even if under an alias. It was only a matter of time before the account was somehow associated with my true identity.

This brings up a scenario which I encounter often. A client needs to disappear, is ready to start using an alias during travel, but does not want to give up those hard-earned hotel points. I do my best to convince them that free stays and upgrades are not worth the risk. Some listen, others do not. If necessary, I encourage them to use up all the points with their family at a posh resort and get it out of their system. We can then start over when they return. Others absolutely insist on maintaining their status while using a different name. This is possible, but not advised.

Hotels do not allow you to transfer your points to another person. However, they allow you to update the name on the profile if you experience a name change. This is most common after a marriage (or divorce), but they also allow any type of legal name change. I am not suggesting my clients change their names (more on this later), but I have assisted one client who really wanted to keep the points. He downloaded a name change form from his state, completed all the fields, and submitted it to the hotel chain. The legal paperwork was never processed through any government entity, it was just sent straight to the hotel. They accepted it and updated the name on the account. Again, this still associates you to your alias, and eliminates most of the privacy of using an alias. I do not recommend this technique.

Places to Avoid

If I want privacy, I avoid fancy hotels and resorts. There was once a day when the rich and famous could enter the Ritz Carlton and expect a private and discreet experience. Today, prestigious entities present more privacy invasions than the smaller chain hotels. The following presents several scenarios I have witnessed on behalf of myself and clients.

- In Los Angeles and New York City, paparazzi stage in front of posh hotels hoping to photograph a celebrity. I have walked into a Holiday Inn with a household-name celebrity and no one noticed. I try to avoid places frequented by photographers with no morals.
- At fancy resorts, staff are trained to memorize the names and faces of all guests. They are also instructed to greet guests by name at all times. Loud echoes of “Hello Mr. Bazzell” any time I walk out of my room are not desired.
- Some resorts advise their staff to research guests in order to make small talk. While at a resort in Grand Cayman during a keynote under my real name, a beach concierge with whom I had never met asked me how the weather was in South Dakota. I don’t think he knew what a PMB was.
- While at a beach resort in an alias name during a privacy consultation with a wealthy client facing death threats, I was approached by the pool concierge. She stated, “It is great to see you again Mr. (alias)! I can’t believe it has been two years since your last visit!” I don’t believe that she remembered me. I suspect she was told my name by other staff, researched my past stays in the internal computer network, and then attempted a conversation which would make most people feel special. The only thing she accomplished was to convince me I needed to change up my alias.
- While checking into a resort, the staff demanded to know my flight number for my departing flight. I was using an alias at the hotel but my true name during air travel. I provided a false number, and was immediately told it did not exist. I conducted a quick search and provided the details of a different flight. This sufficed until staff arrived at my room at 7 a.m. to escort me to checkout in order to make my flight. I should have paid more attention to the departure time of my alias flight.

Overall, you are watched, monitored, and tracked more in expensive resorts than any other short-term lodging option. These are all minor issues to most, but could be devastating to someone trying to disappear. This provides numerous opportunities for an adversary to identify your room number by simply following you and listening to employee chatter. I would never consider placing a victim in this situation. I prefer the anonymity of standard hotels where the staff cares very little about your presence.

Rental Homes

You may need to rent a home indefinitely or while you are purchasing a house. The methods for each are identical. When I need to find a rental home for a client, I insist on the following.

- The house or unit must be independently owned. Large apartment companies will demand a hard credit check and valid SSN from the applicant. This is a deal-breaker. Independently-owned buildings possess owners who can make their own decisions without following a policy manual. Cash can also influence a landlord.
- Utilities must be included in the rent. This often leads to higher overall costs, but better privacy. I will not need to convince the power company to accept an alias name without DOB and SSN in order to activate service. We will tackle that later with a home purchase, but included utilities is optimal while renting.

I always start my rental home hunt through traditional advertisement avenues. I avoid Zillow and other online options. These tend to cater to larger rental companies or individuals with numerous properties. These scenarios often lead to meetings with property managers on behalf of the owners and an immediate application including background check and credit pull. Instead, I start with newspapers.

I found my first apartment in the classifieds section of a local newspaper. This may show my age, but that was the only option back then. Today, many modern rental offerings avoid printed distribution, especially when the internet provides a broader reach. In my experience, the perfect landlords are those who still advertise in the papers. I try to seek out those that have only one or two rental units and prefer to place signs in the yard instead of hiring property managers to recruit tenants. A later chapter tells a true story of working with a private landlord in order to hide a client. Until then, I will include a few notes about the process.

Background checks and credit pulls are off limits. Some may believe that these inquiries do not attach the client to the future rental address, but I disagree. Services such as Experian's Tenant Credit Check and others ask for many sensitive details such as the name, DOB, SSN, and previous addresses of the prospective tenant (the client). These details are also demanded from the landlord. Experian will possess full rental histories of previous tenants from this landlord who chose not to protect their privacy. Therefore, Experian already knows the likely address of the rental unit. They can easily associate the client with the address before the credit report is created. This data is then shared with other divisions of this data mining empire, as well as the next inevitable breach.

My ultimate goal is to never reveal the true name of the client to a potential landlord. Once I find a property suitable, I make direct contact with the owner. I explain that my client is a domestic violence victim and is scared to tell anyone where she lives. When I encounter a

landlord who has no empathy for this, I move on. I always offer a cash deposit and first month of rent, as well as the promise of a cash monthly payment in advance. This goes a long way. In dire circumstances, I have offered up to six months cash in advance for the luxury of anonymity. There is no magic to this. You simply need to find the right property owner. Cash is king. It will provide more negotiation power than you might expect. My experiences with a client which are explained later will provide much more detail.

In 2020, I began using my business in order to ease the process of finding short-term rental homes for clients. I established an “anonymous” LLC for this purpose, obtained an EIN, and opened a checking account. I always keep a packet of LLC documentation ready to show a potential landlord. This includes the certificate of organization, confirmation of EIN from the IRS, recent bank statement, and LLC checks. This new method has worked amazingly well, and was created after a conversation with a friend who travels long-term for work at various refineries. I asked him how he handled rental housing, as I know he relies heavily on cash while on the road and can be gone for six month stretches. He advised that he never arranges or pays for rental homes because his employer handles all of the logistics. This changed how I look at rental homes for clients needing three to twelve months of temporary lodging. My first test was in January of 2020 when a client requested assistance leaving an abusive situation.

She located a small home for rent by an independent landlord which included utilities. I asked to see the home and met with the owner. I advised that I owned a small company and needed temporary housing for an employee who was relocating to the area and was having trouble finding a home to purchase. I stated that my business would pay the rent and eagerly provided all of the paperwork mentioned previously (none of which included my name). I encouraged the owner to verify my business details with the IRS and the bank. I also offered a “proof of funds” letter from the bank disclosing the current balance to settle any fears that the owner may have about getting paid. I offered to write a check for the first and last month on the spot and agreed to go to a local branch of the bank, if he desired, in order to verify the check. The owner agreed to rent the home directly to my LLC with very little interest of knowing the employee’s name. He was more interested in my line of work. I told him I managed finances for wealthy people and my new employee was in training for a similar position. Technically, this was the truth. I do receive payments from wealthy people for various services, and I would be teaching my client ways to replicate my process for her own benefit.

Since this experience, I now have a better understanding of the overall tactic. Most landlords assume that a business is less likely to stiff them on rent than an individual tenant. They also hope that future rental opportunities may exist from my business. Best of all, I now use these positive experiences whenever an owner wants a reference. I recently witnessed a potential landlord call a previous landlord asking about my LLC as a renter. After their quick conversation, I wrote a check and received keys to the home. Neither of them knew my real name. Much of this technique involves confidence, manners, and respect toward the owner.

Hidden Cameras and Unauthorized Entry

Regardless of whether you are in a hotel, Airbnb, rental home, or any other type of lodging, you should be aware of hidden recording devices and unauthorized access to your living space. In the past two years, I have had two clients who were surreptitiously recorded nude in hotel rooms and extorted for money over the recordings. Due to pending civil litigation, I cannot speak about those specific events. However, I can explain a typical extortion process which has recently impacted hundreds of victims nationwide.

The typical hotel customer provides his or her real name, home address, personal email address, and cellular telephone number during the registration process. By now, you know that this is risky behavior. However, I suspect that over 99% of all hotel guests have no concerns about privacy and willingly hand over these details. This information can be used against you when a rogue employee wants to contact you with threats of releasing sensitive content. Consider the following fictional example, based on true events.

- The night manager of a hotel is a creep and installs a small hidden camera in the bathroom of a few empty rooms. He places the devices behind some folded towels, in a tissue box with a pinhole, or within the shell of a smoke detector.
- The device is battery powered and recording is enabled by motion sensitivity. A micro SD card stores any video recorded.
- You check into this hotel under a real name and email address.
- The night manager assigns you to a room he knows to possess a hidden camera.
- You enter the room and change clothes and shower as normal.
- You check out the next day.
- The manager arrives for his shift and enters the empty room you were assigned. He replaces the SD card and inserts the original in his computer.
- He downloads the videos of you nude.
- He searches the customer log and identifies your name and email address.
- He sends you an email from a private account and includes an excerpt of a video displaying you nude in the shower. He threatens to send a copy to all of your friends and family if you do not pay him money or send self-created nude videos.
- You refuse to respond and he publishes the video to dozens of porn sites. He includes your full name within the description. A Google search of your name reveals these videos.
- He locates you on LinkedIn and identifies the names of your co-workers.
- He sends copies of the videos to people within your employment circles. He spoofs an email address to make the message appear to have been sent by you.
- He repeats the process as often as he receives new videos of new victims.

Does this sound ridiculous and far-fetched? It absolutely happens. Search “hidden camera found in hotel room” within any search engine, video website, or social network and you should be presented with plenty of evidence documenting this popular extortion technique. Using an alias is an important step to thwarting this behavior. It does not prevent the capture from a hidden camera, but it prohibits most of the extortion. If you used an alias name and email, the offender will think that is your real information. If he threatens to post the videos with your name on them, no one will know it is you. If he threatens to send the videos to friends and family, he will find no one connected to your alias name. This is only one level of defense toward this type of behavior.

I encourage all of my clients to conduct a thorough sweep for any hidden cameras within all temporary lodging situations. This includes rental homes, as some landlords have been caught spying on tenants. The procedures for identifying hidden recording devices varies from amateur solutions to expensive gear. I will outline my recommendations, beginning with simple and free methods.

- Visually inspect all areas of each room.
- Look for any inappropriate small holes within objects facing the shower or bed.
- Search common areas such as tissue boxes and clock radios.
- Search behind all towels in the bathroom.
- Look for holes drilled into plastic smoke detectors or walls.
- If your room has one brand of fire alarm devices throughout, but a different brand plugged into an electrical outlet, this is suspicious.
- Turn off all room lights and identify any LED lights emitting from devices.
- Always travel with a roll of electrical tape. Cover any suspicious holes or lights.
- Unplug the alarm clock and place it in the closet.
- Inspect all vents for suspicious devices.

If you discover anything which appears to be a hidden camera, choose your next steps carefully. First, personally document your findings with photos and videos. Next, contact the police and file an official report. Allow them to retrieve the device and maintain control of it as evidence. Never complain directly to the hotel staff. This could result in destruction of the device and a cover-up. If you are a high-profile target forced to use your real name upon check-in, immediately request a different room after you are assigned a specific room. If a rogue employee has assigned you to a room with a known hidden device, demanding a new room on a different floor may provide a small layer of protection.

Personally, I always travel with a small amount of gear which assists in quickly identifying suspicious devices. There are a plethora of affordable “hidden camera detectors” online, but I find most of them to be useless. Some have reported that viewing the cell phone camera

through the front-facing screen while the lights are out will reveal covert lenses, but I have found this to be unreliable. I now rely on two pieces of hardware any time I stay in temporary lodging.

The first is a Milwaukee Spot Infrared Imager unit. This device was recommended by my friend and former colleague Tom Gibbons, and was discussed on my podcast with him as a guest (Episode 119-How to Find Hidden Recording Devices). This handheld device displays heat sources. Any small camera will possess some type of power and will generate heat unique from surrounding areas. This unit costs \$200-\$300, but there are more affordable options on Amazon. I will warn you that you get what you pay for with these. If you care enough to search for this type of privacy invasion often, bring the best equipment.

The next device which is always in my travel bag is an old Android mobile phone which possesses the open-source privacy app **Haven** (guardianproject.github.io/haven). Haven is an Android application that leverages on-device sensors to provide monitoring and protection of physical areas. Haven turns any Android phone into a motion, sound, vibration and light detector, watching for unexpected guests and unwanted intruders. Before I explain the usage, let's focus on the installation and device selection.

Fortunately, I possess numerous old discarded Android devices from my government days. These are outdated by today's standards, but will function appropriately for our needs. I have tested Haven on a Samsung Galaxy S4 and various versions of the Motorola Moto G series. First, conduct a hard reset to the device, wiping all data and restoring it to the factory default. You can find details for this specific to your device online. Next, install the Haven app from the Google Play store. If you have a rooted phone with a custom ROM, which was explained earlier, you can also load this app from the F-Droid open-source app store.

Once Haven is installed, scroll through the welcome screens. Select the “Configure” button and accept the default value for each option. You can tweak these settings later if needed. Optionally, add a telephone number for notifications via Signal. I do not use this feature as I do not care to receive remote notifications or connect this device to my Signal account. Your threat model may demand this level of protection. Exit the settings to the main Haven screen.

Please note that this device will only be used for this single purpose (monitoring a room). It will never possess a SIM card and will only use public Wi-Fi. This is a Google hardware device and privacy is always a concern. It should be turned off when not in use and never be present in your home. Therefore, I accept the privacy violations of Google in order to gain the benefits of this app when needed. Please consider whether you need a device like this in your life before jumping in. I also use this Android device to bypass check-in at hotels which offer the ability to unlock the room door wirelessly from the app.

Once you are at the main Haven screen, which will likely display a view from your front-facing camera, choose the settings icon. If desired, enable Video Monitoring and exit the settings menu. Selecting the “Start Now” option on the main screen enables monitoring. The camera will detect movement, the microphone will detect noise, and the internal sensors will detect movement of the device. Begin monitoring and test the settings. When you make a sound, you should see that indication on the home screen. When you move anything in front of the camera, it should detect this activity. You can safely turn the screen off and your device is now monitoring the room.

In a typical situation, I enable all options whenever I leave my hotel room. I place the device propped-up on the desk, leaning against something, in the room while plugged into a power source for charging. The front camera faces the bulk of the room. When I return, I stop the monitoring application and choose the “View Logs” option. This presents any triggers during my absence. This includes any images and videos collected from the camera, audio recordings from the microphone, and notifications if the device was moved. If housekeeping enters the room, I will see video evidence of this and any associated audio files. This small device will let you know when someone entered your room. Further, it allows you to see and hear their actions. This is a powerful tool.

It could also be considered illegal in some situations. A few states in the U.S. are considered two-party states in regard to audio recording. Both parties (you and the people being recorded by your device) must consent to the recording. If housekeeping or anyone else in the room does not know about the recording, they do not consent. This could place you in a criminal situation and must be considered. Furthermore, some other countries have very strict laws about surreptitious recording of any sort. You do not want to be placed in detention in China for such a violation. I have a solution that works well for me.

When I am staying in a hotel, my Android device with Haven installed is always monitoring while I am away from the room. I carry a small laminated placard which states “DO NOT ENTER, RECORDING IN PROGRESS”. I place this on the outside of the entry door. This notifies housekeeping of my desires for no one to enter. It also serves as a deterrent to anyone with malicious intent. It indicates that someone is in the room, and this may not be the best burglary target. Finally, this notifies anyone who may enter that a recording device is present. In most situations, this waives any consent issues.

If you chose to enable remote notifications via the messaging application Signal, you can receive the audio and video from your monitoring before returning. This can be beneficial in case you are notified of a threat which would make you stay away from the room. In extreme situations, this app could make you aware of a physical threat from miles away. Imagine if the app displayed video of an intruder hiding under the bed or hotel staff hiding a camera in the ceiling of your room. Again, these scenarios may sound far-fetched to you. For my celebrity

clients, it is more common than most would think. Haven does not work on iOS, but I am fine with that. I would never want this app on my primary communication device. It works best on old phones which can be left behind in your room without worry about theft. Please become familiar with the app before relying on it in a real scenario.

In closing this chapter, I hope that you now have an interest in protecting yourself while away from home. Each layer presented here has an impact on your privacy. Alias names, eavesdropping identification techniques, and intentional monitoring solutions will keep you safe from both random and targeted attacks. If you are considering an escape from an unsafe situation, please start with the following considerations.

- **Plan well, but secretly.** Only tell trusted people about your plans, and only if they truly need to know. Save enough money for your escape without generating suspicion.
- **Wipe your tracks.** Clear any internet search history on any computers which can be accessed by your adversary. Do not leave with any mobile devices previously used. Change your passwords to your email and delete any communication which might reveal your new location.
- **Collect the essentials.** Make sure you possess enough clothes, medicine, and any other requirements to get you through the first stage of your escape. Store this somewhere private and secure until time to leave.
- **Possess all necessary documentation.** Make sure you have your real ID, passport, birth certificate, and anything else in your name. Plan to never return to your abusive environment and possess all essential documents and paperwork required to prove your identity and access any financial accounts.

International Considerations: Many readers have reported difficulties using alias names while traveling in countries other than America. I have also witnessed resistance from hotel clerks demanding to copy my passport. Many foreign countries have rules which require hotels to retain a copy of official identification from each guest. This can be quite invasive. I do not have a magic solution for every situation, but I provide the following experience I had at a Hilton in London in 2018. Upon arrival at my hotel, I advised the clerk that I wished to check in, but had a question to ask first. I explained that I just arrived in London, and that I left my passport at the airport during customs screening. I further explained that I had received a text message stating that my passport was found and that it would be delivered to the hotel the following day. I asked specifically if the hotel would accept the package and hold it for me. This was a ruse, but it set the scene for my inability to show ID. I offered her my secondary credit card in my alias name (which was used to make the reservation), my Hilton rewards card in my alias name, and my “employee ID” from the company I own, also in my alias name. She happily accepted these items, made a copy of my credit card, issued my room key, and assured me that the staff on duty the following day would deliver my package. I suspect she forgot all about me within an hour, and I never provided a copy of my passport.

CHAPTER TEN

HOME PURCHASE

This entire book has been preparing you for this chapter. I believe the single piece of information which should have the most privacy protection is your home address. This is where you sleep, where your family spends time, and where you are most vulnerable. If someone wants to harm you, it will likely be at your home. If a reporter wants to question you, he or she will stake out at your house. If you take no action to protect these details, you will be on hundreds of people search websites within ninety days after purchase of a new home. You will be a single Google search away from complete exposure.

I mentioned a few scenarios previously where you may want to hide your home address. As I am writing this, there is a Reddit thread asking for the home address of Congresswoman Alexandria Ocasio-Cortez. In the first response, the full details of her apartment are legally presented. Last month, an online gamer was “swatted” by police when a competitor spoofed a call to 911 claiming a home invasion in progress at the gamer’s address. Last week, a lottery winner was bombarded by members of the press at his home demanding to know what he would do with his millions, while exposing his address to the world. This week, an “Anti-Vaxxer” contacted me because a person with opposing views encouraged Facebook users to send hate mail and “Molotov cocktails” to her home address. Recently, a stalker was arrested for breaking into Taylor Swift’s New York apartment. Next week, will someone have an interest in finding you?

We live in an entitled world where everyone believes they deserve access to everything. If you have received public attention for an unfortunate event, protesters believe they deserve the right to scream at you while you try to sleep. If you are publicly involved in a civil lawsuit, journalists believe they have a right to bother you at home at any time desired. I believe things will get worse, and we should be proactive in protecting our address. Because of this, I never purchase a home in my real name, or in the name of a client. I use trusts, LLCs, and nominees to hide the true identity, and I do this while obeying the law. This chapter will be intense at times, and I do not expect every reader to apply all tactics. I present several options as I go, and anything you do to protect your information helps. I also discuss a few of my failures, which are often the best education. I ask that you take a moment and question your own level of threat. Is it at all possible that an adversary may try to find you? Is there any scenario where having a public home address could backfire on you? If either answer is yes, I hope you consider an anonymous home. We cannot predict the future. Once an undesirable incident unfolds, it is too late to hide. You simply must be proactive.

Home Search Considerations

The first step toward obtaining your private home is to consider the overall location. You may already know the general area where you want to live, but there are privacy implications everywhere you look. If you have flexibility within the exact area you wish to purchase a home, you should consider the following.

County vs City: In populated urban areas, there can be many privacy benefits to living immediately outside of city limits. Cities usually have more requirements for various licenses and permits. Everything from pets to parking requires personal information, and most will be placed within insecure databases. Counties, especially unincorporated areas, often have fewer requirements.

Occupancy Permits: Some cities and counties require occupancy permits that identify every individual that resides in the home. Providing false information to this government entity is likely a crime. Avoiding the mandatory disclosure will bring unwanted attention to your home. A call to the local housing division should expose these requirements.

Government Presence: I also look closely at the overall level of government presence within the community. While numerous free government services may be welcome to those who desire them, they come at a cost to our privacy. I pay close attention to the presence, and therefore demand, of law enforcement. When I see police cars constantly present in a specific neighborhood, it tells me two things. First, this is likely a high-crime area. Second, there is an increased risk of being involved in a traffic stop or police report, which can become public information. I look for quiet areas without the need for much government presence.

Neighborhood Involvement: I always look at the overall level of involvement of the local residents in the neighborhood. When I see a subdivision with an active Facebook page, I become concerned. This is an outlet for people to complain about their neighbors and speak poorly about others behind their backs. When a new person moves into a neighborhood such as this, especially someone who tries to be private, it usually sparks interest and investigation from people that have nothing better to do.

HOA: Homeowner Associations can be very invasive to new residents. I try to avoid them at all costs. Some HOAs require all new owners to submit full details of all occupants and registration information for any vehicles. This is likely improperly stored and eventually shared with the entire neighborhood. Many HOAs possess leaders that abuse the limited authority they believe they have. Some force you to pay annual fees via personal check, and refuse to accept cash. While you may have success providing alias information, the constant scrutiny is unwelcomed by most.

Next, you should consider the method for your home search. Real estate professionals can be very helpful, and I will discuss choosing a proper representative in a moment. However, you will still need internet search resources. I always recommend conducting your own searches for a while before committing to professional help. This will give you a sense of home prices and areas you wish to target. There are some important considerations when using sites such as Zillow and Redfin.

All real estate search sites will push you to create a free account. This will allow you to save searches and receive alerts after registration. However, an account is not required in order to use the services. I encourage people to keep their own notes and never create an account. These sites contain powerful analytics that track users. The information collected about your home preferences, IP address, third-party cookies, and provided details creates a very unique profile, which is valuable to data mining and marketing companies.

Whether you choose to create an account or simply search “anonymously”, there are some best practices. Always use an isolated browser which is not connected to any personal accounts. You could install a secondary browser such as Brave, and only use it for home searching. Do not sign in to any other services, especially email accounts and social networks. This isolation will prevent some personal data leakage. If you only wish to possess a single browser, such as Firefox, you can take advantage of Firefox’s Multi Account Containers to separate home search traffic within a designated container. As previously stated, this is probably overkill since Firefox introduced “Total Cookie Protection”.

Next, you will likely need a real estate professional during your search. The internet has given us most of the tools we need to find a home, but the viewing, negotiation, and closing processes are still easier with professional help. Since real estate commissions are usually paid by the seller, there is little reason to do this on your own. However, use caution. Many real estate representatives are pushing clients to sign contracts guaranteeing a commission. If you choose a house for sale by owner, you may be required to pay your chosen representative a percentage of the sale price. If the seller does not agree to the commission, you are on the hook. I never commit to real estate help until I have found the right person and the right contract. Many reputable representatives will not require a contract until you are ready to make an offer. This varies by location.

Choosing the right person to aid in your home search is very important. This is not the time to simply hire the last person you met who was showing an open house you visited. Because you will be purchasing the home anonymously, you need experienced help. When I am searching for a real estate professional (not all of them are “agents” or “brokers”), I start with an online query. I search for the styles of homes which interest my client. Next, I make a list of candidates who are selling these homes. I then read reviews and eliminate anyone that seems

to constantly generate negative comments. From there, I contact each via email (the proper address to use is discussed in a moment) with the following message.

"Hello, I am new to the area and looking to purchase a home in the near future. Your online reviews were great, are you accepting new clients? If so, I will be purchasing under the name of a trust. Do you have experience with this? Can you disclose any of your experiences or any nuances with purchasing under a trust in _____ county? Thanks!"

In my experience, this will generate three types of responses. The first will be no response at all. You may seem difficult right away and not worth their time. Good, weed those people out. The second response is a canned message telling you how great they are and asking you to schedule an appointment. This may be acceptable, but only as a last resort. If you emailed enough people, you should see a third type of response. It will be very specific, directly answer your questions, and display confidence in the ability to title a new purchase in the name of a trust. This is the type of person we want. Schedule a couple of house-viewing appointments and see how you feel about the relationship. This person will be heavily involved in your home purchase.

My next test is to identify the person's willingness to assist in my quest. I first ask which title company they recommend, and then follow with, "What are their requirements to title into trust?" If the real estate representative reaches out, finds the answers, and provides the information to you in a timely manner, I place them ahead of others. When a person does not put the effort to provide clear answers, they are out of the race. I am looking for a person willing to do their homework.

Everyone knows someone who is associated with real estate. When you disclose to friends and family that you are house shopping, you might be bombarded with referrals. These should be avoided. When you contact a friend of a friend that is a real estate agent, you just lost all anonymity. Your real name will be entered into the provider databases and there is now a trail from you to the home you choose. I believe your chosen professional should never know your real name. That may sound harsh, but consider the following.

A client allowed a friend to be the buying agent on her behalf. The home was placed into a trust and her name was not present on the public county records. She placed the utilities in the name of the trust and did a great job of remaining private. Her friend entered my client's real name and details into the database owned by the large national chain realty association. After the purchase, my client began receiving junk mail at her home, addressed to her real name, asking her to refer others to the business that helped her during the purchase. A month later, she began receiving unsolicited mail offers for appliances and exterior cleaning services. The buying agent's company sold their customer list to third parties. My client is now exposed,

and can never fully repair the damage. If you want a truly private home, you must watch every step and never disclose your real name to anyone associated with the sale.

Let's assume that you have found a few homes you want to view and you have identified a real estate professional with whom you want to start working. Before you meet, you should have several things in order. I will list these individually including considerations for each.

Email: When you contact real estate professionals, assume that everything you provide to them will be shared publicly. They will register your email for unsolicited messages and share it within various marketing systems. I always create a ProtonMail email address for the sole purpose of the home purchase. It does not identify my name or the trust name. I keep it generic such as home.purchase@protonmail.com. The name associated with this account, which will be seen by recipients, is also generic such as "Homes". This is the only email I will use during the entire process, including closing paperwork. It will not be used anywhere else.

Phone: Your hired professional will want your phone number. This will also be entered into the databases owned by the company and shared with numerous third parties. I designate a VOIP number for this, and choose an area code associated with the general location. I will never use this number for any other personal purpose. I expect this number to become public.

Name: In my early attempts at purchasing an anonymous home, I was very restrictive over any information divulged to anyone. I found that telling someone, "I would rather not give you my name", was not well received. It also caused extra awkwardness during every encounter. I no longer do this. Instead, I am Michael Johnson. I keep it simple. No one has ever asked for identification during the house hunting process. This will happen closer to the closing, and we will deal with that later.

Current Location: Everyone wants to know where you currently live. Much of this is small talk in order to seem polite, but some is to identify the type of location you may desire. I always have a story ready for this. I usually go with, "I am renting in (nearby town) while I look for a new place". I avoid anything exotic such as Hawaii or anywhere else mildly interesting. If you get pushed for a specific address, have a nearby hotel address ready to go.

Current Employment: One of the first questions you will hear from your house hunter will be, "What do you do?". Again, this is small talk, but anything you say will be documented somehow. Most successful real estate professionals add this to your profile and use it when they need a reference from a specific industry. I recommend keeping it simple. I usually go with, "I work from home as an accountant. It's pretty boring, I add numbers all day". There is rarely a follow-up to this, and you just set the scene that someone will be home at all times when you move in. This can be a burglary deterrent when questionable subjects start asking about you.

Business Cards: In 2021, I assisted a client purchasing a new home. She struggled with small talk and had great difficulty presenting herself under an alias name. My solution for her was business cards. I created a generic card which contained her alias name, occupation, email address, and VOIP number. Any time someone asked for her details during her home search, she just handed them a card and said “It may be easier if you just keep this”. This action immediately stopped all questioning, which relieved my client. I find the printable options sufficient for most needs. I use the cards from Avery (amzn.to/385p4zF), which are quite affordable. These can also be convenient when meeting neighbors.

Personal Interests: In general, I hate this type of small talk. Questions such as, “What do you do for fun?” are used to form a relationship. If I say that I play baseball, the other person believes he or she must mention baseball on occasion in order to build my trust and close the sale. This is typical in all areas of sales. I just say, “I’m doing it now!” and move on. I caution people to avoid saying too much. While it may seem acceptable to disclose your passions for classical piano and vegan food, you just made yourself quite a large needle in a small haystack. Keep it simple.

Faraday Bag: This one may be a bit on the paranoid side, but consider your cellular telephone usage while viewing homes of interest. If you subscribe to the 2-phone plan presented previously, you may want to prevent your device from connecting to cellular towers near your future home. This is especially true if your device is registered in your real name. When you enter a home address into your mapping application for directions, this is stored forever within some platforms. If you buy the home, in which you entered the address into your phone, you now have a small yet permanent connection from your device to your new home. I prefer to meet with my real estate people at their office, and then either ride with them or follow them in my own vehicle. My mobile device is in a Faraday bag during the entire hunt. If I want a photo of something, I ask my agent to photograph and email the images to me.

Social Engineering: My last piece of advice is to rely on old-fashioned social engineering when necessary. If questions start to become invasive, turn them around and get the other person talking about themselves. When I am asked, “What is your rental address?”, I reply with, “Hey, that reminds me, what do you think of the Tempe Heights neighborhood? Do you live near that area? Where would YOU move to?”. That should get them on a different track. This can be applied to practically any topic. When asked, “What do you like to do on the weekends?”, I return a question of “What is there to do around here? Where do you hang out?”. This may take some practice, but will go a long way in your future of being private.

Home Choice Considerations

In regard to choosing a home, most of this decision will simply be personal choice. When I am assisting a client with a history of domestic abuse, I want him or her to feel safe and have some extra security protection. If my client is well-known, I may place more priority on privacy. Regardless of your situation, I ask you to consider the following issues.

Privacy from neighbors: Most people that reach out to me for help buying a home anonymously have a strong interest in privacy. I first look for privacy fences and windows which do not expose the inside to a direct view from the street. I don't want the interior to seem like the outside is watching in. Big windows and glass doorways are nice, until they are a security and privacy risk.

Garage to hide vehicle: Possessing a garage is vital for any home I will consider. This has nothing to do with the security of the vehicle(s). A properly garaged vehicle does not expose license plates to public view. Attached garages are best, as a vehicle can be loaded for a trip without the neighborhood knowing you are packing.

Interviews: This plays a large role in my selection of a home. The residents surrounding a home can give quite an indication of potential problems, or lack of. I usually conduct a search of the neighborhood on people search sites, identify the residents, and take a look at their social networks. This gives an overall vibe of the community and may identify any bad apples. Researching police reports online is also beneficial. If your area does not provide this, strike up a friendly conversation at the local police department and ask about that specific area. Finally, I place a lot of emphasis on my own "street walk" around the neighborhood.

When I was conducting my street walk for a client in northern Arizona, I encountered a neighbor mowing his grass. I asked if I could step on his property and we had a brief conversation. I asked about the neighborhood as a potential buyer, and he had nothing but great things to say. It turns out the vacant home for sale was the issue, and the entire neighborhood saturated local police with every witness of a drug sale or physical altercation at the residence. The problem-residents finally moved due to the pressure from a proud neighborhood. When searching for a home for a violence victim, I welcome concerned neighbors that are not afraid to get involved. My final question was, "What were their names?" The man responded, "I have no idea, we keep to ourselves for the most part out here, until you cause trouble". Perfect.

You can make any home private with anonymous titling, but you cannot magically make it secure from the burglars on your street. I typically place more emphasis on the surroundings of the home than the house itself. I care more about feeling private and secure than the drop ceilings or hardwood floors. Always take your time and keep these things in mind.

Radio Frequency Monitoring

When I found the home I wanted to purchase, I had one last piece which needed attention. I wanted to know the types of police calls received in that neighborhood. I could access police calls for service and partial reports through the city's website, but those never tell the full story. I wanted to hear for myself. This is why I always spend a couple of days monitoring police radio frequencies for the area. There are two ways to accomplish this.

I like to program a portable police scanner with the frequencies of the departments or divisions responsible for all calls for service within the area of the home. I rely heavily on **Radio Reference** (radioreference.com) to provide the information I need for programming. I then leave the scanner on in my vehicle while I explore the neighborhood. If I can receive the transmissions from my current lodging, I leave the scanner on throughout the day.

I am listening for the types of calls and consistency of interaction. If I hear officers taking reports of vehicle burglaries every morning in the target neighborhood, that is concerning to me. If there seems to be a high number of drug-related arrests, that may influence my decision. However, if most of the calls are vacation checks, business checks, and other proactive patrol scenarios, this is a good sign.

Any time I hear officers doing anything proactive within the community, this tells me that staffing is appropriate; crime is manageable; and an overall desire to protect residents exists. Meaningless public statements from a department's Facebook page should not convince you that an area is safe. Use your own eyes and ears to make your own informed decision.

Possessing a physical police scanner may be overkill for your needs. For most clients, I recommend an online service called **Broadcastify** (broadcastify.com). This free service allows you to listen to live emergency radio frequencies from anywhere in the world. I can be in Los Angeles but listen to real-time calls in New York City. The service relies on radio enthusiasts throughout the world. They configure their own radio equipment to scan a specific set of local frequencies and then broadcast the audio stream through Broadcastify.

Paid members can access historical recordings of any station. You could listen to the previous night's activity the following day. This is very beneficial for hearing the busy midnight shift without staying up all night. I maintain a paid membership at all times. It allows me to retrieve recorded audio of my own neighborhood after I hear about a possible prowler several days or weeks later. It is very affordable at \$30 per year.

Home Purchase Considerations

Assume now that you have found the ideal house. You have already established a trust as previously explained. You have a person you trust to serve as your trustee, preferably with a common last name different than yours. You have a notarized certification of trust at your disposal, which is signed by your trustee. You are ready to make an offer, and it is time to jump in and commit.

During my initial explanation of my anonymous home strategy, I will assume you are paying cash. I know this just upset some readers. While most of my wealthy clients have spare cash to throw at a problem, the rest of us do not. I start with cash purchases because they are the easiest. I have never had any major obstacles in these scenarios. At the end of this section, I will discuss hurdles that enter into a home purchase when obtaining a mortgage. These will vary depending on your location and lender, but you have options in all situations.

The original offer and earnest money are fairly simple. The contract can be created using digital-only services such as DocuSign, and all of this will be performed by your real estate representative. You can state that you want the offer to be in the name of your trust, and that your trustee will digitally sign. You can use your previously given email address in order to receive the links to the online documents. The earnest money can almost always be in the form of a cashier's check. This is usually a 1% deposit based on the offer price. If you back out without an acceptable reason, the seller can keep this money.

In 2021, I encountered one title company which required the deposit to be submitted electronically via wire. This is not a huge deal, just not ideal. I explained that I had already purchased a cashier's check, but agreed that the remaining funds would be submitted electronically. This was allowed, but I expect more scrutiny in the future.

A cashier's check does not identify you or your account and it is usually held by the chosen title company. The DocuSign electronic documents will arrive via email, and require the trustee to click "I accept" a few times. In optimal situations, the signature line only identifies the trust at this time, and not the trustee's name. You can specify this to your representation, but it is not vital. The trustee will be publicly exposed during closing anyway.

I prefer all DocuSign contracts to be delivered to a ProtonMail email address created specifically for this purpose. The email address will become public information and I do not want anything associated with a personal account. I create a free ProtonMail account for this purpose which can be accessed by multiple people if necessary, such as a spouse and trustee. Does your trustee need to be the person who clicks on the approval button for the documents? Legally, yes. However, it would probably never be scrutinized if you completed this formality. Use your best judgement.

Before I move on, I encourage you to research the title company before you commit to an offer. In many cases, the seller chooses the company to use, but you can request a different option if you are uncomfortable with the selection. I always call the chosen title company and ask the following questions.

- Can the deed be placed in the name of a trust?
- Does the trustee's name need to appear on your internal documents?
- Does the trustee's name need to appear on the county deed?
- What documents will you need?
- I have a certification of trust, will that suffice?
- Is there any specific wording you need on the certification of trust?
- Can my trustee sign from a remote location?
- If you demand a "wet" signature, can this be notarized and sent via overnight mail?
- Will anyone need to be present at the closing?
- When do you need funding?
- Do you accept a cashier's check for earnest money?
- Do you accept a cashier's check for the final balance?

I am looking for acceptable answers and an overall confidence in their ability to title a home in a trust. I have found a few title companies that were completely incompetent, which caused more problems for me. As the buyer, you have the power in this sale. Make sure you are comfortable with the title company selected for this transaction. They work for you, and you have the power to find a better option. I typically call three title companies before I make a choice.

Some sellers will require a proof-of-funds letter. With a cash purchase, this is a document created by the bank holding the funds confirming that a specific amount of money (determined by you) is currently available in the account. I try to avoid these with the initial offer, but I am never surprised to see the request on the final acceptance. If this is required, I will explain bank accounts in trust names in a moment. If securing a loan, this is a document created by the lender acknowledging pre-approval for a specific amount.

After some negotiation, an offer is usually accepted by both the buyer and the seller. There will be several digital "signatures" during this process, all in the name of the trust, and preferably without the trustee's name. Some title companies will insist that the trustee's name is present, and the line will read similar to The Home Buying Trust, John Wilson, Trustee. This is acceptable, as this information will be needed at some point regardless. These documents should stay fairly private, but this data will be used for public documents eventually. Please revisit "Choosing a Trustee" in the legal infrastructure chapter before you commit to someone.

Assume that you now have a contract for the house. The rush for inspections begins, and you need to schedule numerous people to visit your potential new home. This can feel quite invasive to a privacy-conscious person, and I see many people make numerous mistakes at this point. Any company that is hired will demand information from you. Furthermore, they will contact the title company and retrieve any details that it possesses. The service companies will abuse this data by sharing it with third parties, and you have almost no say in the matter. Anything you provide will eventually be public information. Approach with great caution, and consider the following incident which happened to a client in 2018.

My client hired a local home inspection service to inspect the entire house. She found a company with great reviews and felt confident in hiring the service, which she found online. The inspection company used a service called Porch for all reservations and billing. These online services make it easy for the contractor to focus on the job and not the logistics. While convenient for the workers, it is a privacy nightmare for you. The following five excerpts were taken directly from the porch.com privacy policy website.

“We may share your information when you consent or direct Porch to do so. Depending on the circumstances, consent may be expressed (i.e., you specifically agree either verbally, in writing or electronically) or implied.”

“You consent to be contacted by these parties by telephone, email, mail, text (SMS) messaging, fax, or other reasonable means at any of the residential, cell or fax phone numbers or addresses you provide, even if they are listed on a national ‘do not call’ or ‘do not contact’ list. You agree that these communications may include prerecorded, artificially voiced or autodialed telemarketing messages, and that they may be monitored and recorded for quality assurance and other reasons.”

“From time to time, we may partner with third parties to offer discounts, rewards or other programs or promotions. We may disclose the personal information of the participants in the programs to those business partners. ...We will disclose your personal information to those business partners when you consent to that disclosure, including consent implied by your agreement to the applicable program rules.”

“We may decide to sell, buy, merge or reorganize our own or other businesses, conduct a securities offering, or do a joint venture or other strategic transaction. We could also be involved in a bankruptcy, liquidation, dissolution or similar transaction. Any such transaction may involve disclosing personal and other information.”

“We may share aggregated, non-personal data with service providers, advertisers or existing or potential business partners.”

In summary, any information provided can (and likely will) be shared, sold, given, traded, or lost to any company that may have interest in you as a new homeowner. Deals like this are the reason that we all get bombarded with unsolicited mailings in relation to home ownership when we move into a new house. While some may enjoy the promotional material, we have a more important concern. The more your name and address are shared with marketing companies, the faster your information will appear publicly online. If you want to keep your name and address private, you have two obligations.

The first is to avoid companies like this. My client was able to track down a direct telephone number for this inspection service and politely requested to book an appointment directly. Instead of citing privacy concerns, she stated she was not tech savvy and couldn't figure out the website. The service obliged and conducted the work, submitting a paper invoice and happily accepting cash for the job. The second obligation is to expect every provided detail to be publicly released. Therefore, you will only provide the name of the trust as the customer. If you receive grief for this, tell the provider that the trust is paying for the work, and your name being present could delay payment.

Once the title company starts doing their work, they will probably request to see the entire trust document. This is an extreme violation of your privacy, and they may "record" it with the county. Remember, the entire trust outlines you as the grantor and beneficiary, and your desires for asset distribution when you die. No private or government organization should ever need that entire document. That is the purpose of the certification of trust as explained earlier. Provide a notarized copy of the certification of trust to your representation to give to the title company. The title company may also request a Statement of Authority signed by the trustee. This will be a form specific to each company, and allows them to continue their work in good faith that the trustee approves all of these actions. This may specify the address and timeline, and is acceptable. All of the future digital signature documents will likely display the trustee name after these documents are provided.

This brings up another important point. You should never need to deliver anything directly to the title company. In my purchases, I never step into a title company's office. They do not know what I look like. By not being present, you cannot be tricked into signing something or displaying identification. Allow your real estate broker to earn their commission and do all of the leg work.

Assume now that the inspections are acceptable and you are ready to proceed with the purchase. A closing date will have been set by the title company, and they will demand the remaining money to cover the purchase price of the home. I now present purchase protocols for both cash and loan transactions. Let's start with the easiest option of purchasing a home without a loan.

Anonymous Home Purchase (Cash)

When paying in cash, I always recommend providing the funds a few days prior to the closing date. Some title companies want the check to “clear” before approving the transfer, especially when the situation is unique. This brings us to the next dilemma. How do you pay the title company anonymously? This can get a bit tricky. The official answer is that you can never have 100% anonymity when buying a home with cash in America, even with the use of a trust. The exception might be homes under \$25,000, but that is not very applicable to our situation. This is because there is always a paper trail of the financial exchange. You cannot show up with \$300,000 in 100-dollar bills and walk away with the keys. Any check, even a cashier’s check, can lead back to you. Therefore, our desire is to be PUBLICLY anonymous. If the IRS wants to prove you bought a specific home, they will succeed. They have the power of court orders to financial institutions. If a private investigator or journalist tries to determine your home address, we can make that extremely difficult, if not impossible.

When I began assisting with anonymous home purchases in 2015, I was able to present a cashier’s check for practically any amount. This check was issued by the same bank that my clients used for personal accounts, but the check number was not directly associated with the client. The bank could disclose transaction data if provided a court order, which would identify the client, but the title company would have no details about the client’s account. This worked for a couple of years until wire transfers became the mandatory procedure. Today, practically every title company will demand an electronic wire transfer for amounts over \$25,000. Most companies claim this is due to fraud, but wire fraud is more abundant than check fraud. I believe that title companies demand wire transfers because it provides less liability than a check. It is easy to immediately confirm a transfer with the issuing bank.

I have given up my fight to provide a cashier’s check for the home purchase. My last success was in 2017, and it was quite a struggle. Today, the only sales which accept cashier’s checks are auctions of foreclosed properties. I see many bidders bring numerous checks in various amounts, such as \$25,000, \$50,000, and \$100,000, in order to make immediate payment. There is less scrutiny on these lower purchase prices. When purchasing a home through a more traditional process, I provide the final purchase amount via wire transfer from a new account created in the name of the trust. This should be done with much thought, and please consider the privacy implications before submitting a wire.

A wire transfer is an electronic transfer of money. A traditional wire transfer goes from one bank or credit union to another using various computer networks. In order to send a wire transfer, you need specific instructions directly from the recipient (title company). These details are given to your bank, and the wire transfer request is prepared. You may be charged a small fee, and the transfer is almost immediate without a hold on the funds.

You must identify the account which will provide the funds. If you have the entire purchase price sitting in your personal checking account, a wire transfer can send the money straight to the title company. However, this process will also send your name and account details. Any information provided to the title company is likely to be filed with the county, and can become public record. Therefore, this is a bad idea. My preference is to create a new account within the name of the trust.

It can be convenient to ask your current personal bank to create a secondary account for your trust in order to send a wire transfer from it instead of your personal checking. This can be a mistake. Consider the financial risk company Early Warning. Early Warning delivers payment and risk solutions to financial institutions nationwide. In 2017, I requested my own consumer report from them. It clearly identified all of my checking, savings, and investment accounts. It easily connected all of the accounts to me, and provided details for every deposit, withdrawal, and payment associated with each account. Early Warning shares this data with over 2,500 financial institutions and unknown third parties. In other words, this company knows when you add an account, all payment details including wire transfers, and historic balances since the account was opened.

My preference is to open a new account at a local credit union in the name of the trust. This should be done in advance of placing an offer on a home. While this institution may participate in systems that share account details, there will be a degree of separation from your personal accounts. Your procedure for this will vary based on the trustee of your trust. There are two routes I recommend.

- If YOU are the trustee of your trust, you can create this account yourself. You will need to provide your DOB, SSN, and identification. Make sure the account is only in the name of the trust, and that your name does not appear in the title. This account is obviously associated with you, but could be used as a layer of privacy protection when only disclosing the name of the trust.
- If SOMEONE ELSE is the trustee of your trust, you cannot open the account yourself. Banks and credit unions will want to see the trust documents and will only allow the trustee to create the account. Obviously, they will want the DOB, SSN, and government identification from the trustee. This can be very uncomfortable for a trustee, unless it is a close family member or spouse. Consider making yourself the trustee before opening the account, and then amending the trust to assign someone else as trustee during the closing process. This will be explained in a moment.

Both of these options may seem sloppy and they both possess privacy exposure. Neither are perfect, but they may be your only options. I cannot guide you toward your best choice, but I can offer a detailed example of the actions taken by a recent client. I have included a modified timeline to show the approximate dates when each step was taken on the following page.

- January 1, 2018: My client created her trust, assigning herself as the trustee and beneficiary.
- January 2, 2018: My client opened a checking account, in the name of the trust, with a local credit union. The account is associated with her SSN. She complied with all Know Your Customer (KYC) laws. Instead of the entire trust document, she only provided the certification of trust. She deposited enough funds to pay any potential earnest money requirements via a cashier's check from another bank.
- January 10, 2018: My client identifies the home she desires, places an offer from the trust name only, obtains a cashier's check in the name of the trust from the trust checking account as earnest money, and digitally signs the offer in the name of the trust without a specified trustee. The offer is accepted.
- January 11, 2018: My client transfers the approximate funds required for the complete purchase from the bank associated with her personal checking account to the new trust account, via cashier's check, from the original bank. This will require 2-3 days to clear.
- January 15, 2018: My client is informed of the final amount due to the title company to purchase the home and is given wire transfer instructions. She verifies the deposit into the trust account. The payment is due before the closing date on January 30, 2018.
- January 16, 2018: My client provides the wire transfer instructions to her credit union. A transfer for the final purchase price is issued and received at the title company. She made sure that only the name of the trust appeared on the wire, and that her name was not present within the digital transaction.
- January 17, 2018: My client amends her trust and assigns the role of trustee to her niece, who is a trusted family member with a different last name.
- January 20, 2018: My client's niece provides a real "wet" signature on the title company's statement of authority document and my client provides a notarized copy of the certification of trust document declaring her niece as the trustee, and signed by her niece. These two documents allow the niece to digitally sign at closing.
- January 30, 2018: My client's niece remotely executes the digital signature for the closing and my client now owns the home.
- January 31, 2018: My client amends the trust, re-assigning herself as the trustee. Some may choose to postpone this until utilities are activated.

As another reminder, I am not an attorney. In this situation, my client created and controls her trust. She made herself the trustee in order to open a checking account in the trust's name. This will be beneficial during utility activation. Before signing any paperwork with the title company or providing trust documents, she assigned her niece as the trustee. This gives the niece the full power to sign on behalf of the trust. The only name the title company knows is that of the niece. The client is still invisible to the title company.

Anonymous Home Purchase (Loan)

The previous section has been simplified, demonstrating a successful execution with a cash purchase. There are always hurdles faced throughout an anonymous home purchase. The biggest roadblock you will face is when obtaining a loan for a home. You are now at the mercy of the lender in regard to titling the home in the name of a trust. Be selective about your choice of lender. During the initial conversation, advise that you wish to place the home in the name of your trust for estate planning purposes. The first response will likely be positive, but you should push the issue. I recommend the following series of questions to a potential lender.

- **Can I place the home in the name of my trust at the time of purchase?** This wording is important. Some lenders will insist you place the home in your name at the time of purchase with the option to change the deed to the trust after purchase or after the loan is repaid. Titling your home in your name for a single day is enough to expose your address to the internet forever. Most lenders agree to this without verifying with the companies to which they will resell the mortgage.
- **Can the trustee be someone other than myself?** This will be met with resistance. I have witnessed larger lenders reject this while local banks allowed it. If you want to completely keep your name off the county record, it helps to have a trustee other than yourself. Make this requirement clear from the start, and expect to be denied.
- **Does the trustee need to be a co-signer of the loan?** Many lenders which have allowed a third-party trustee later demand that the person be listed within the loan. This is unfair to the trustee and is inappropriate. Obtain a clear answer on this now.

In most situations, your lender will allow you to title the home to the name of a trust, but will demand that you are publicly listed as the trustee or beneficiary of the trust. This is not ideal, but still provides many privacy benefits. If I know your address or the trust name, I will be able to verify through the county that you are the trustee. However, searching your name on the county site should not identify the address. Only the trust name is searchable and will be abused by third parties. Being your own trustee eliminates some anonymity, but that may be required to purchase your home. Titling to a trust simply makes you harder to find.

Overall, a lender will know everything about you, including your SSN and DOB. In order to give you a line of credit, a hard pull will be conducted on your credit history. They will know the address of your home and the name of your trust. However, they will probably not share these details publicly. The concern is a breach or third party which has access to this data. This is why I focus on smaller credit unions and banks. Ask whether the institution resells their loans or keeps them in-house. The latter will place much less scrutiny on the use of a trust. Paying with cash will always be easiest and most private, but possessing a layer of privacy by using a trust during the loan process is also helpful. For most clients, the goal is to stop home addresses from being published on the internet. This can be accomplished, even with a loan.

Tax Record Exclusion

I have had a handful of clients which possess an affiliation with law enforcement who desire privacy in regard to public property tax records. If your home is titled in your real name, many counties offer an option to request these details be hidden from public view. This requires completion of a specific form and a letter from your employer stating that you work in law enforcement.

The only time I recommend this is when you will not be placing the home into the name of a trust. If you are purchasing an anonymous home, I believe this option is an awful idea. In a way, you are making yourself a larger target. A rogue employee, or poor security protocols at the county offices, could expose you and your address. Furthermore, if you are the only home in your neighborhood with missing tax records, you must be someone special. I much prefer proper titling into a trust. You then need no additional “protection”, which may actually backfire on you.

USPS Issues

In 2018, I helped a client purchase an anonymous home in a rural area of Missouri. After he moved into the home, he realized there was no mailbox on the property. He soon discovered that the entire neighborhood collected mail at one central group of mailboxes further down the road. These boxes required a key, which my client did not possess.

A call to the post office resulted in a demand for a list of occupants. This was met with immediate concern from the client. I have seen this many times, and the solution has been surprisingly easy. I recommend having your trustee contact the local post office. The trustee should state that he or she is not currently residing at the property, but that someone can be sent to the local office with the closing paperwork from the title company clearly identifying the trust and trustee name. The owner can then take in these details without the need to provide any type of identification.

Since the USPS is a government agency, we want to be cautious to never lie or give inaccurate details. Showing them the closing paperwork, identifying the full name of the trust and trustee, should be sufficient to add these details to the local carrier's roster. In my experience, possessing the original closing paperwork is enough to be given a key to the mailbox. I encourage the trustee to be listed on the USPS roster in order to accept any mail in that name. Often, property tax bills and utilities will be mailed to the trustee's name instead of the actual trust. The next hurdles include utilities and various home services. The next chapter will present numerous solutions to keep your name out of marketing systems which sell your data.

Children

Children present a new hurdle in the desire for an anonymous home. If your children are home schooled, you likely have no issues. If you reside in an urban area with competitive schools, this could present concern. Many schools demand proof of residency in order to eliminate children from other areas who are trying to avoid their own troubled schools. Overall, I recommend registering your children within the appropriate schools local to your home. However, do not provide your actual home address. This will be placed into many records, including some that will likely become publicly available online. I have found county schools to be much less restrictive about residency requirements than city schools. You will be constantly pressured to provide your home address, and the following ideas may buy you enough time until they stop requesting your personal details.

Obtain a local UPS box and provide that address as a street address. If questioned, state that you are in the process of building a home in a nearby neighborhood. Make sure your actual home address and the UPS store address are both within the boundaries for the chosen school. This keeps your actions legal. If asked where you are staying, provide a hotel address within this same area, and clarify that you want the UPS address used for all mailings. In my experience, you will only receive resistance if that school is strict about blocking non-local students from attending. Make sure that the school you choose is also funded with your property tax payment. This provides additional legal compliance if you should ever be accused of fraudulently enrolling your child into a specific school.

The use of a legal guardian, such as a grandmother, may be appropriate for you. A child can be associated with a legal guardian within school records and that person can sign documents when required. This may not offer a strong layer of protection, but could keep you off school records which will likely become publicly available. In my experience, private schools are much less demanding about home address verification, as they are directly funded by you. Most private schools do not have a specific residency requirement, and will accept a UPS address as the primary residence.

Bringing children into an invisible home can carry many more issues into your life. This will likely generate several long discussions about cellular telephone usage, internet habits, friends in the home, alias names, employment, and the protection of the details you have hidden. I hope that the overall lessons within this book assist with these discussions and decisions. I can assure you that many of my clients lead invisible lives, even with children in the home. This will require more effort on your behalf, but the work is worth the reward. As an added bonus, creating privacy awareness with your children at a young age may provide many future benefits once they obtain their own independence and enter the world of data mining, credit abuse, and numerous other privacy violations.

Neighbors

Most residents in your new neighborhood will want to get to know you. They likely have great intentions and simply want to be good neighbors. While some may be nosier than others, everyone in your neighborhood is a potential threat toward your privacy. I may not take this harsh of a stance if it were a pre-internet era. Today, we are at risk of online exposure everywhere we turn.

During the home selection process, I mentioned how I monitor Facebook groups in order to identify potential problems before moving into a neighborhood. These same groups are now a threat toward your anonymity. Your neighbors will post any gossip they hear within these groups and use them as an outlet to vent frustrations with other neighbors. My best advice is to stay off the minds of these people. Don't speed through the neighborhood, keep your property maintained, and keep to yourself. These three suggestions will keep you out of the majority of the drama within online groups.

The next concern is new privacy invasion companies such as Nextdoor.com. Nextdoor is a social networking service for neighborhoods. Users of Nextdoor submit their real names and addresses to the website and posts made are available only to other Nextdoor members living in the same neighborhood. The premise seems like it offers a small layer of privacy by allowing people to communicate with neighbors without the content being publicly visible to the rest of the internet. However, I am very concerned with the amount of detail being collected by Nextdoor. First, let's look at three excerpts of the privacy policy.

- “We share information with service providers, affiliates, partners, and other third parties where it is necessary to perform the Member Agreement, to provide the Services, or for any other purposes described in the Policy.”
- “We may share your personal information with certain third-party service providers to help us operate, provide, improve, understand, customize, support, and market our Services.”
- “We share some aggregated information about our neighborhoods with government agency members and other organizational members.”

In other words, much like every data mining company in America, they have the right to do practically anything they want with your information. After moving into my anonymous home, I received a letter in the mail from Nextdoor. It was an invite to join the group assigned to my neighborhood, and it specified the neighbor (full name and address) who requested Nextdoor to contact me. This already felt invasive, but I played along. I assumed this would be a great opportunity to learn more about my neighbors and apply some disinformation about myself.

The invite included a specific code which allowed me to join Nextdoor without providing address verification. I entered the code on the Nextdoor website, and it immediately populated my entire home address (but no name). The code was unique to my house. Nextdoor then demanded to know the name of the primary occupant of the home. I entered J Doe, and I was declined. An error message notified me that the system required a full name in order to complete the registration. I entered John Doe and was declined again. I was informed that real names must be entered, and I began to wonder how people would join if their name was really John Doe. I settled on John Williams and I was allowed to proceed.

Nextdoor asked me to complete a profile about myself which included interests, hobbies, and my overall reason for joining Nextdoor. Fortunately, there was an option to skip all of these. They then requested the full names and email addresses of all occupants, which I skipped. I was then prompted with a screen telling me I needed to invite one friend to Nextdoor, and I was offered the option for Nextdoor to connect to my contacts in order to easily select someone. I skipped all of this.

Nextdoor then displayed all of the local addresses in my neighborhood which had not enrolled in the service, and asked if they could send invite letters to each of them on my behalf (disclosing my full name and address). Skip. Finally, they pushed me to install the Nextdoor mobile app (in order to collect more details from my device), which I declined. By default, all local users now see the email and full address in my profile.

I realize I am a bit paranoid, but this smells like a data mining company to me. Imagine all of the extremely accurate information they receive from the occupants of a household which is not available anywhere else. I suspect that we will see this data emerge into other people search companies. The email address I provided for my profile was unique to this service. I eagerly watch for it to appear within other online repositories. I will update this on my podcast if anything should surface.

I never posted to the neighborhood group on Nextdoor, but an announcement was made that I had joined. The entire group received a public message on the community wall stating my full (alias) name and street of residence. I then began receiving unsolicited messages ranging from “Welcome to the neighborhood” to offers for home improvement. Reading through the comments, I observed the usual offenders. Most were people complaining about speeders and ugly properties. On one post, the commenter identified the license plate of a vehicle which upset her, and a response identified the name and address of the owner. These groups are your next threat, and can quickly unravel all of your privacy strategies protecting you.

While updating this chapter in April of 2020, I logged in to my Nextdoor accounts in order to identify the ways in which communities were embracing this technology during the COVID-19 pandemic. I was not surprised to see posts shaming neighbors, including full names and

addresses, who were not “social-distancing” correctly. However, most of the content was for the purpose of spreading unverified information and conspiracies associated with the area surrounding my neighborhood. It was a mess.

Because of the popularity of online groups such as Nextdoor, which allow abuse of collected data, I ask you to consider what information you will provide to your new neighbors. Expect that any details could become public within an internet group. If you upset someone, do you want your full details shared with other neighbors?

I insist on always providing an alias name and backstory to my neighbors. They all call me John. They believe I travel the country applying software patches to large commercial heating systems. I am boring to them and they do not think of me often. It does not change my relationship with them, but it makes me worry less when someone decides to mention me on the internet. No one knows my true name or background.

I stay away from any neighbors fueled by drama. If I am mentioned or documented within their social networks, the data will not compromise my privacy as it will not be accurate. This may seem extreme to most. However, there are no “re-dos” when sharing personal details with a neighbor. Anything provided will be repeated, embellished, and exposed. Choose wisely.

Finally, always remember the amount of effort which was required to obtain your private home. I doubt you want to unnecessarily repeat that process with a new property because of a small mistake which disclosed your true identity. Spend considerable time creating your new alias which will be presented to neighbors. Rehearse and repeat before “going live”.

If you already created a Nextdoor account and want your personal data removed, you must first deactivate the account and then request deletion. I took the following steps once I knew I did not want to participate within the platform.

- Navigate to <https://nextdoor.com/deactivate/>.
- Select any reason desired.
- Deselect “Share this feedback with your neighborhood Lead(s)”.
- Click “Deactivate”.
- Navigate to <https://help.nextdoor.com/s/contactus>.
- Under “I have a question about”, choose “My residential account”.
- Under “Relating to”, choose “Deleting my account”.
- Click “I still need help”.
- Create a message demanding deletion of your account and removal of all content.

Nomad Home Ownership

You may have some confusion about how the privacy benefits of nomad residency, as explained previously, can be combined with home ownership. There are countless scenarios which legally allow nomad residency while owning a home, and likely as many which do not. I am not an attorney, and I could never acknowledge every unique situation, but I have opinions on many common scenarios which I encounter often. I ask you to consider the following situations which I have witnessed during consultations with clients.

A client became a nomad through South Dakota while leaving an abusive relationship. She eventually decided to purchase a primary home in South Dakota. The home was titled to a trust and her name was never associated with the purchase. She is employed in South Dakota, and her employer only knows her PMB address. She is legally a South Dakota resident and has no issues with the government by only using the PMB address. This could be replicated within Texas by using a PMB provider such as Escapees.

A client became a nomad through South Dakota. She later purchased a home in California, titled to a trust. She lives in this home full-time and owns no other properties. She never rents another home or lodging. Eventually, California will demand that she become an official resident or face steep fines. Legally, she should become a California resident and surrender her South Dakota license.

A client became a nomad through South Dakota and traveled the world in an RV for two years. He later purchased a home anonymously in Washington, but kept the RV. He continues to spend winters traveling through southern states and a few months in summer at his home in Washington. As a full-time traveler, he meets the requirements of nomad residency from South Dakota and calls his RV his “home”. Washington does not have a state income tax, so he would not need to file a tax return to that state for any income earned while inside the state.

A retired client became a nomad through South Dakota and later purchased two homes in the name of his trust in other states. He does not spend more than a few months per year (total) in either home. He travels most of the year. He chose to keep his South Dakota nomad residency and calls his PMB “home”. If pushed by either state of his homes, he could prove he spends minimal time in that state.

A client became a nomad through South Dakota. She later purchased a home in New York, titled to a trust. This is not her “primary” home as she travels often as part of her employment. She spends more nights away from her home than inside it. She calls South Dakota her domicile state. She spends much of her time in California as an actress, but owns no property there. Both California and New York could argue that she should be a resident of their state.

She files a California tax return to claim her California income. She never works in New York and files no return there. This is a bit of a grey area, and should be discussed with an attorney. Remember that you technically do not “own” your home. Your trust or LLC owns it, and you are the beneficiary. However, you should be cautious of state income taxes. If you earn money while physically inside a state with income tax, you owe your share. I have many clients who are legal nomads but spend much of their time in tax-aggressive states such as California. They make sure to possess a CMRA mailing address in California, and use it on their state tax returns, which claim all income earned while in the state.

Personally, I never recommend home ownership, even titled to a trust, in states such as California and New York, while trying to maintain nomad residency in South Dakota. It will catch up to you and you will face legal scrutiny from state government. It is simply not worth the risk or hassle. If you plan to live full-time within any state, you should be a resident of that state. If you can justify nomad residency due to extensive travel or multiple homes and an RV, then you may qualify. Don’t make this decision lightly.

In my experience, states without income tax on wages such as Alaska, Florida, New Hampshire, Nevada, South Dakota, Tennessee, Texas, Washington, and Wyoming are less concerned with nomads being in their states. High-income states such as California, Hawaii, Illinois, New Jersey, New York, and Washington D.C. are always looking for residents who are not paying their share of state taxes. If you purchase a home in a non-nomad state, research the driver’s license address requirements and apply the lessons throughout this book toward that situation. Most states simply want their tax, transportation, and other revenue from their residents. Keep them happy and live your anonymous life without scrutiny.

Purchasing a home “anonymously” can be quite difficult. I often see clients struggle with this. I recently advised a couple which were quite concerned with the entire process and their ability to complete the various steps without making mistakes. They did not plan on making the purchase for another year, but wanted to be prepared. I encouraged them to conduct a trial run, knowing they would not buy anything at this time.

They contacted a real estate professional; toured some homes; provided their aliases; and asked many questions about the specific process of purchasing a home in the name of their trust within their desired county. There was less pressure on them since they knew they could make mistakes. It also helped them learn more about various local neighborhoods.

My clients did well during their practice. They never disclosed any personal details. Some readers may be unhappy with me for potentially wasting the time of the real estate professional when my clients knew they would not buy any of the houses toured. Several months later, when they were ready to purchase, they re-contacted the same real estate agent and found a home. The commission was earned.

Selling Your Home

While you can get away without an SSN during the purchase of your home, it will likely be required when you sell it. This is because the title companies are required to report income from a home sale and must associate it with a specific SSN or EIN. The IRS requires you to pay taxes on income from a home sale if it exceeds a specific threshold. Most people are exempt from this taxation if the home was their primary residence, but title companies will insist on an SSN or EIN for the submission. I don't worry much about this, but I have a few rules for myself and my clients.

First, I only place a home for sale once I am completely out of it. I do not want strangers inside my home without me being present. I do not want any real estate professional to have access to my home at any time thanks to digital locks which can be opened with a smartphone. Once I am gone with no plans on living in the home again, I no longer care about the number of people entering and viewing the house.

Once I have moved to another anonymous location, I have no objection associating my name and SSN with the purchase of the previous home. I sold my house in 2015 which had no connection to me. It was in the name of a trust. During the closing process, I provided the trust documentation disclosing me as the beneficiary. My trustee provided a fresh signature. I provided my SSN to the title company for the check to be issued and confirmed a trust checking account associated with my true identity. There is now a trail from me to the residence, but I no longer live there.

Some may be worried about tax issues upon the sale of a home. The profit you make on the sale of your home might be taxable, which is known as capital gains taxes. This is why the title company will demand the SSN of the seller. The IRS typically allows you to exclude up to \$250,000 of capital gains on real estate if you're single and \$500,000 if you are married and filing jointly. For example, if you bought a home 10 years ago for \$200,000 and sold it today for \$800,000, you would have a profit of \$600,000. If you are married and filing jointly, \$500,000 of that gain might not be subject to the capital gains tax, but \$100,000 might be.

This exception to capital gains taxes has a few requirements. The house must have been your principal residence; you must have owned the property for at least two years (there are some exceptions to this); and you must not have claimed the \$250,000 or \$500,000 exclusion on another home in the two-year period before the sale of the current home.

Always contact a tax professional to understand your unique scenario.

Complications

Purchasing an anonymous home in America can present many complications, but is almost always possible. Some countries possess stronger privacy laws which do not make owner information public, and decrease much risk of associating your home to your true name. Some countries insist on documentation of the owners and occupants of every home, which can present more concerning problems. Please use the methods presented here in order to identify equivalent privacy strategies within your own country if needed.

I have never encountered a country which forbid home ownership by an entity such as a business or trust. If you do, consider the use of a trusted nominee for the documentation, but pay close attention to all fine print. Stay legal, but stay private. Most countries simply need a “face” to the purchase. They want a documented human being who has the authority to make the purchase with funds. They also want someone to hold accountable in the event bad things happen on the property.

I have witnessed rare situations where a state demands to know a trust’s beneficiary or director during the home purchase process. These demands are typically enforced by the title company. While an estate attorney can help you navigate this intrusion, consider the following. An LLC can be the beneficiary of a trust. As the grantor of a trust, you can temporarily assign another person as the director before closing, and reassign yourself as director after. We can usually find privacy strategy loopholes any time a state begins to tighten their controls. This strategy exceeds the scope of this book, but information is plentiful online.

Finally, any future homes should not use the same trust as any previous houses. A new home is a perfect opportunity for a fresh start, and allows you the freedom to disclose your true identity with any previous purchases. Since the names of each trust, along with previous and current addresses, will be publicly available, someone could match your old home with the new house if the same trust is used. While this is unlikely to happen, do not take any shortcuts. The extra effort of establishing a new trust is justified. Expect to encounter your own unique hurdles during your home purchase. Your two biggest issues will be purchasing while obtaining a loan and insuring the property. I explain options for the latter in the next chapter, but loan companies will aggressively try to convince you to avoid titling in the name of a trust. Stand firm on this requirement and force them to work with you. Remember, home loan companies earn a lot of revenue from your monthly payments. Make them work for it.

Final Thought

As I updated this chapter, I was following the aftermath of the U.S. Capitol siege. Numerous FBI agents and countless amateur internet sleuths began hunting the people captured on video during the event. I learned about David Quintavalle. David is a retired firefighter from Chicago

who was identified by members of an online community called Reddit as the man visible in numerous online videos striking police officers with a fire extinguisher. The internet mob began calling his home and threatening his family. He was labeled a terrorist by his neighbors. Individuals even showed up at his home to torment the household members. He was reported to the FBI and forced into an interrogation. The problem is that David was not present at the siege. He was shopping in Chicago at the time (and kept his receipts as proof). An online stranger compared images of the suspect to David's Facebook photos and determined they depicted the same person. Without any vetting, the attacks began. A week later, the suspect in the videos was identified as Robert Sanford and arrested. However, David still receives threats, and police officers continue to monitor his home. If you do not place photos online, you cannot be wrongly compared to criminals. If you title your home in a trust, your address cannot be easily searched online. If you prevent your home from any association to your name, you can stop internet mobs and journalists from confronting you at your home. David did nothing wrong, but continues the fight to clear his name. Don't let this happen to you.

Typical Client Configuration

A summary of this chapter was previously provided, but I believe I should present more details here. During an anonymous home purchase, I typically advise the following.

- Open a checking account in the name of the trust associated with you as trustee.
- Prepare a computer for anonymous online home searching.
- Meet with a home search specialist without providing your true name.
- Select your desired home.
- Amend your trust to appoint a new third-party trustee.
- Provide a Certification of Trust signed by your trustee to the real estate professionals.
- Provide a Certification of Trust signed by your trustee to the title company.
- Provide earnest money for the deposit via check from the new trust bank account.
- Complete all inspections in the trust name.
- Provide full purchase price to title company via bank wire from the trust account.
- If purchasing with a loan, have the funds wired under the name of the trust.
- Have your trustee digitally sign all documents before closing.
- Have your trustee manually sign closing documents in front of a Notary.
- Send all closing documents via certified mail.
- After purchase, establish utilities in the name of your trust or LLC.
- Establish home insurance in the name of the trust associated with your true details.
- Establish a local mail receiving option.
- Create rapport with your neighbors under an alias name (if desired).
- Never associate your home address with your true name.

CHAPTER ELEVEN

PAYMENTS, UTILITIES, & SERVICES

Assume that you have purchased your home privately. You have a “safe house” in which you can sleep well at night, without worry of any current or future adversaries showing up unannounced. You have completed a vital step, but now you have many smaller hurdles to conquer. Eliminating your name from the county records and public deed prevent much of the online scraping of public information. However, utilities and services are your next enemy. The moment you provide your name and SSN to a utility company for a “soft pull” of your credit, these details, including your new address, are shared with numerous data mining companies. I tested this in 2015.

I had just moved into a short-term rental which had no association to my real name. A former colleague owned the home, which had been vacant. I paid cash in advance and he handed me the keys. I only planned on staying a few months, so I was not extremely concerned with long-term privacy. I set up anonymous utilities, as explained here, with the exception of the power company. This was in California, and the power company was a government entity. This city provided its own power services. I was a bit new to the extreme privacy game and I was cautious not to provide any inaccurate information. I activated service with my true name and DOB. Within 60 days, my home address appeared associated with my name on a consumer information report available to third-party credit companies. I was burned. I expected this, and didn’t think much of it, as I was moving soon. Today, I would never repeat that mistake.

If you are not diligent about possessing anonymous utilities, your hard work purchasing a private home will have been wasted effort. Many power companies, insurance providers, and household services supplement their profits by sharing customer data with third parties. My rule is to never associate my true name with my home address in any way. This includes any service that has a connection to my home. This chapter will explain several options to help you create your own anonymous payments strategy.

First, we need a way to make anonymous payments. I recommend a multiple-tiered approach. You should always have numerous options for payments available at any time. I have placed them in order of most desirable to least.

- **Cash:** This may seem obvious, but cash is your most anonymous payment source. I recommend that all clients maintain a steady supply of cash in the house in a secure location. Any service that accepts cash should receive it as a priority. Most clients make monthly trips to a bank branch a few cities away and make a withdrawal large enough to meet the demands for the month. I never suggest visiting a bank branch within or near your city of residence. This creates a pattern that can identify a great starting point to find you. Personally, I only withdraw money while traveling, and almost always outside of my home state. Cash leaves no digital trail, aside from video surveillance and fingerprints.
- **Prepaid Cards:** In previous books, I spoke highly of a specific line of prepaid cards. Today, I do not have much preference. These will only be used for in-store purchases, and never online. In order to use any prepaid card on the internet, you must first register the card to your SSN. If you only use them in stores, no registration is required. I look for cards that are NOT reloadable, and display wording similar to “gift card”. I prefer options which can store at least \$500 to minimize the purchase fees for each card. Prepaid cards leave no absolute digital trail to you if purchased with cash, aside from video surveillance, fingerprints, and transaction histories. Transaction history is stored forever, and purchases with the same card can be identified and analyzed. In a moment I will explain how this compromised a client.
- **Privacy.com:** This is a requirement for me and almost every client. This free service allows you to possess unlimited unique debit card numbers which can be attached to a specific vendor. Payments can include any name and billing address desired. Full details will be explained in a moment. There is obviously a connection to you, but it is not visible to the merchant.
- **Trust/LLC Checks:** Limited use of checks can be beneficial. Your bank can issue checks with the LLC or trust name without your name appearing anywhere. This creates a strong trail to you, but may be required on occasion, as detailed later. These are directly connected to your SSN, but the merchant does not see this association.
- **Secondary Credit Card:** This may exceed the comfort zone of some readers, but it can be helpful when a true credit card is required. This was previously mentioned in the temporary housing chapter, and will apply to a few payment strategies. I will discuss additional related options in this chapter. This is the least private of all options, as the number is identical to your personal credit card number. Credit agencies will have immediate access to this connection, as will merchants if you use both personal and alias cards.
- **Virtual Currency:** The cleanest way to make an anonymous purchase is to use virtual currencies such as Bitcoin. If properly obtained and spent, there is practically no way to be identified. I explain many important considerations within this chapter.

Prepaid Cards

There is a common misconception about prepaid credit cards being anonymous. While they can offer a great layer of privacy, any digital card payment is going to leave some trail. I am very cautious about the original purchase location and any use near my home. It is also vital to keep possession of all cards, even after the balance has been spent. Leakage of the card or account details can immediately expose your purchase history and could jeopardize the privacy of your home address. I will explain with the following details from an experience with a client in 2018.

An important part of any complete privacy reboot includes continuous testing. You might purchase an anonymous home with 100% success. However, what happens after a year or two? Are you still private? Did your name and address leak onto the internet? By constantly testing our strategies, we can have more confidence that we have succeeded. In this case, my client reached out to me, through her attorney, in order to conduct an assessment of her overall privacy. She lived in a home titled to a trust, and never associated her true name to her address. She followed all of the rules set forth in this book, and was doing everything correctly. Her threat model was high. She had a stalker who went to great lengths to track her. When he found her in the past, he violently assaulted her and destroyed her home. I was happy to see her testing her privacy strategy.

I confirmed with the attorney that I had full consent to attack her privacy strategy in any way I desired. I then contacted her directly and made sure she had truly invited this activity. Once everything was in writing, I began my attempts. I started with the easy stuff, such as people search sites, data mining services, and public records. Even with my inside knowledge of her home address, I was unable to find anything concerning. I then tried to connect a cellular account to her, but was unsuccessful. My attempts to gain access to any digital accounts using recycled credentials failed. It was obvious she had done a great job maintaining her new lifestyle. It was time to step things up a bit, using a recycled tactic that helped in a previous situation.

In 2017, I was tasked with a cheating spouse investigation. I knew the name and address of the target, and my job was to determine if he was having an affair. I purchased a prepaid credit card from a grocery store and shipped it to the target. I claimed that he had won the \$250 gift card when he completed an online survey several months prior. Even if he was suspicious of the story, very few people will turn down free money. This is especially true for people hiding another life from their family. Before shipping the card, I documented the details including card number, expiration, security code, and website to check the balance. I checked the card transactions every day on the card's website. I only needed to provide the card number, expiration, and security code in order to have full access to the history. After a few days, it was used at a Chili's restaurant a few towns away from his home. A few nights later, it was

used at the same place. While monitoring the activity, I saw a pattern of use at the same Chili's every Tuesday and Thursday evening. This was where he was meeting his mistress. I provided this information to a local private investigator who captured photos of the two people eating, and later doing other things in the suspect's vehicle in the parking lot.

I borrowed heavily from this playbook for my new client. A condition of her job was that she must possess a LinkedIn profile, claiming employment from the company which hired her. It is a global company, so she did not need to provide any city or state of residence and employment. However, it was my start. I purchased a \$100 gift credit card and placed it into a "Thank you" card. Inside the card, I wrote a small note thanking her for attending a conference at which she recently made an appearance on behalf of her company. I found evidence of this within an online roster of participants for the conference. I mailed this card to her name addressed to the headquarters of her company. I knew this would cause a delay, but that she would likely receive the card within an internal mail system. Nine days later, I saw activity on the card.

She used the card as payment at a gas station and later a Starbucks. This provided me a general area of her residence. Since I already knew her address, I knew I was on the right track. However, this would not necessarily expose her home if my actions had been conducted by her adversary. I patiently waited until she gave me the single purchase that I needed in order to connect her to her home. After logging in to the card's website with the card details, I saw a new purchase to a pest control vendor. A quick search of this business revealed that they offer in-home pest services such as spraying poisons to kill various critters. A documentation on the purchase made me believe that the card was swiped through a Square branded card reader, which allows people to accept credit card payment with their mobile device while on-site at an inspection. The purchase also displayed the transaction number, which could be used to track the purchase to an account.

I contacted the pest service and stated that I was in charge of purchasing for a small company and was attempting to identify a payment made for pest services. I provided the transaction number visible on the card's history to the employee and asked if she could tell me which property made the purchase in order to update my records. She immediately provided my client's alias name and home address. I thanked her for the time and ended the call. I had made the connection. I had exposed her home address.

You may think this tactic unfair, but her stalker is savvy and would never hesitate doing something like this or even worse. I don't place any fault on her for using the card. I had previously taught her to never use her real credit card for any home purchases and to only use a prepaid gift card or Privacy.com when absolutely necessary. What I failed to stress was the importance of avoiding the use of any gift cards associated with her name in connection to the home. I take full responsibility. She now knows to watch out for this type of attack.

The lesson here is that prepaid credit cards are great when needed, but still carry risk. In most situations, cash could have been used instead. Every credit or debit card maintains a permanent history of all transactions. Even though my client never associated her name with the purchases, I could still see a pattern of behavior. When it was used at the same Starbucks every day for a week, that makes me assume she lives in a specific neighborhood. This could lead me to more intrusive behaviors in order to identify her home. This may all seem far-fetched for some, but these attempts are the everyday reality for my clients.

My client was not upset at the trickery and seemed grateful to know about the potential exposure. On a more interesting note, she now uses this tactic to monitor her young son. She gives him prepaid cards as holiday gifts and monitors the locations where he spends the money. She assures me it is only to make sure he is not visiting shady places or potentially exposing the family any further. You may disagree with this type of behavior, but I respect her freedom to exercise her powers as a parent of a young teenager as she wishes.

My last guidance on prepaid cards is to use them sparingly and erratically. I only use one when I have no cash or cannot pay in cash. I purchase the cards while I am traveling in order to prevent the exposure of my local grocery store. I keep several cards in my possession at all times and label them with my own identification system. The following are examples.

- A “Travel” card which is only used while I am away from home. The purchase history contains transactions from several states and has very little identifiable pattern. It is never used near my home.
- A “Home” card which is only used when absolutely necessary in my home state. I never use it within the city where I live, but I have used it during local outings and errands. It has very minimal use, as I rely on cash when near my home. An example of usage would be a merchant which will not accept cash, such as a local utility. This card is purchased with cash from a local convenience store with an outdated video surveillance system which only stores ten days’ worth of video.
- A “reserve” card with no usage. It is clean and was purchased out of state. It is for emergencies when I need to make a sensitive purchase. If not used within a year, I transition it to the first slot to prevent expiration, and replace it with a new card.

These are just a few ways I have used prepaid cards. It is important to establish your own methods of privacy with which you feel comfortable. Most importantly, know the risks associated with any type of digital payment. In 2020, I observed many retail outlets demanding government ID for all prepaid card purchases. Some stores, such as CVS, even scan the ID and save it. However, other stores, such as Dollar General, typically do not have the hardware to scan IDs. I would never allow any store to scan my ID for any purpose whatsoever. Please use caution and identify privacy-respecting locations.

Privacy.com Masked Debit Cards

In simplest terms, this is a service which provides free masked debit cards which charge back to your checking account. A week rarely goes by when I do not use a new or previously created Privacy.com masked debit card. The reason is that these cards are absolutely free to the user. I currently use this service for many scenarios from one-time online purchases to recurring monthly automated charges. The mobile app and web interface make the generation of new cards extremely easy.

At the time of this writing, registration is open, but only to U.S. citizens. As explained previously, Privacy.com generates unique masked debit card numbers that can be used for online purchases without disclosing your real identity to the online vendor. The purchase is passed through to a checking account on file with Privacy.com, and the funds are withdrawn immediately, as is common with any traditional debit card. Due to increasing pressure from the financial industry, Privacy.com must verify all new users. This will require you to provide your real name, physical street address, and date of birth. This data will be used to verify you against public records. If you cannot be verified, you will not get an account. This is frustrating to privacy seekers, but I understand the necessity due to rampant fraud and federal laws.

The resistance I hear from most people is in reference to the requirement to connect a valid bank account to Privacy.com. Who is to say that the company will not be hacked? I agree that Privacy.com is now the weak link for a cyber-attack toward your account. However, the same could be said about your bank where you hold the checking account. In my experience, your bank is more likely to get hacked than your account at a masking service such as Privacy.com. Therefore, I proceed with connecting a checking account to Privacy.com. However, I do not blindly attach my primary accounts to this service. Instead, I strategically connect a dedicated account that cannot withdraw funds from any other personal or business accounts. This can be done in a couple of different ways.

Many financial institutions, whether traditional banks or credit unions, issue a primary checking or savings account to each member. Secondary accounts can be added under the umbrella of this primary account. These could be checking accounts to isolate proceeds from a home business or savings accounts to encourage various savings goals. While these are all openly connected to the primary account, they each have their own unique account number. A creation of a secondary checking account and connection of that account number to Privacy.com protects any assets that exist in any other accounts. This provides a layer of protection for those concerned about exposing their finances to fraudulent purchases.

Another option is to create a business checking account solely for use with Privacy.com. The negative result with this method is the likelihood of expensive fees attached to a business checking account. I have found that in each of these scenarios, there is usually a minimum

balance that can be maintained to avoid any checking fees. I keep these accounts funded at all times in order to meet the minimum requirement, but not enough to cause a panic if fraud wiped out the account. Everyone's threshold for this will vary.

The best feature of Privacy.com is the flexibility in setting up each card based on what it will be used for. By default, cards are designated as "Merchant" or "Burner" cards. Merchant cards will attach themselves to a merchant (the first merchant to place a charge on the card). Once this has happened the card cannot be debited by any other merchant. Burner cards are single-use and expire after the first charge has been placed on them. These cards should be used for different purposes.

Merchant cards should be used for recurring payments. Since there is no charge for Privacy.com cards, you can create cards and leave them active indefinitely. Attaching to a single merchant is a huge security benefit. If the merchant spills customers' credit card data it will not affect you at all, because the original merchant is the only one who can debit the card. When creating a Merchant card, you can define a maximum transaction limit per week, per month, per year, or per charge. There are reasons to use each of these options. For example, when setting up a utility bill that will be charged monthly, you can use the "per month" option, limiting the total charge amount to what your maximum electricity bill might be. For items like auto insurance which are only billed annually or semi-annually, you may wish to use a yearly or per-charge total instead, setting the limit to your annual insurance rate.

Another important feature of Privacy.com Merchant cards is the ability to "pause" the cards. This allows you to ensure that the card cannot be used unless you log in to Privacy.com and re-enable it by clicking the "Play" button. This is a great feature for cards that are used infrequently on services like online retailers. For instance, you may wish to have an Amazon account, but you might not want the card to always be active if you only use it occasionally. This allows you to freeze the card, ensuring nothing can be billed to it by any merchants.

If desired, you can also associate multiple bank accounts to your Privacy.com account. This is useful if you have several accounts whose transactions you would like to protect with Privacy.com. All of the settings applied to Merchant cards can be changed at any time, with the exception of the merchant. Once the card has "locked" to a merchant there is no way to reverse this. I believe this is a highly desirable feature, as it prevents users from re-using the same credit card number on multiple sites.

Burner cards are only valid for a single transaction. The use-case for these cards is different than that of Merchant cards. Burner cards should be used for one-off purchases from merchants which you don't fully trust; will not use again in the future; or who are likely to implement recurring charges after your initial transaction. As soon as the initial charge is debited from the card, it expires and can never be used again.

When using Privacy.com cards, you can assign any name you like to the card. You can also use any billing or shipping address you like. There are many ways you can use this flexibility. You can use it to order packages to your home without revealing your true name. In this case, you would use the alias name of your choice and your home address as the shipping address (but never the billing address). You can also use it to create disinformation by giving your real name and a false billing address when purchasing online services which do not need shipped to a home. You are limited only by your imagination.

The final customization I like to make to any Privacy.com account is to enable “Private Payments”. This feature is disabled by default. When you make a purchase to Amazon through a virtual Privacy.com debit card number, the transaction on your bank statement appears similar to “Amazon - \$54.03” or “Privacy.com-Amazon”. This discloses the merchant to your bank which provides your checking account. Your bank still knows everywhere you spend money. The “Private Payments” option in Privacy.com allows you to choose one of the following entities which will be displayed for all Privacy.com purchases.

Privacy.com
H&H Hardware
Smileys Corner Store
NSA Gift Shop

While the NSA Gift Shop entry was an option which I jokingly proposed to the CEO of Privacy.com when he was on my podcast, I do not ever use it. I usually choose the Privacy.com option for all clients. This way, all uses of a masked debit card will appear as Privacy.com on the bank statements. Since the bank already knows the source of the transactions, I do not find this reckless. It will remind the client that the charge originated from their Privacy.com account. More important, the bank will not know the identity of the actual merchant for each transaction. If an adversary is in possession of a subpoena for your bank records, or has obtained unauthorized access to your account, no information will reveal the purchase details.

In 2019, I contacted an old friend who now works at a branch of the bank I use for business purchases. I asked her if I could see the details of some transactions on my account, and she obliged. I brought in my statement which displayed only “Privacy.com” and the amount of purchase on three specific transactions. She turned her computer screen toward me, and showed me the full record of the first transaction. It displayed the following details (with my explanations in parentheses).

- Date of transaction (The date which matched my own records)
- Amount of transaction (The amount which matched my own records)
- Privacy.com (The merchant which matched my own records)

- Privacy.com PRIVACYCOM (If I had not chosen to hide the merchant, it would display the merchant name first, such as “Amazon.com PRIVACYCOM”)
- ACH Trace # (844) 771-8229 (The telephone number for Privacy.com)

In other words, the detailed records at the bank did not identify the merchant, such as Amazon, for each transaction. A court order to Privacy.com would obviously reveal this, but partner companies of my bank, and entities such as Early Warning, do not get to see the data.

As with any important accounts, be sure to choose a very strong username and password for your Privacy.com credentials, and enable two-factor authentication through a software token such as Authy. I also encourage clients to “close” cards which are no longer needed. This action permanently closes the cards, and allows you to make new cards for similar purchases. Some users have reported that multiple open cards for the same merchant, such as Amazon, flags the account as suspicious and may cause an interruption. While I have not been able to replicate this, it makes sense to close cards as soon as they are no longer needed.

Once your account is active, you can generate new masked card numbers. These are typically used during online purchases when a customer must manually enter the information. Many merchants may block these cards the first time they are used due to heavy abuse by criminals. I explain more about these scenarios later. If you attach these cards to established accounts with prior successful purchase histories, you should have fewer problems. These masked debit card numbers can also be used in person at many establishments. There is no physical card, so you cannot allow someone else to swipe the card during a sale, but audibly giving the details will usually provide a successful result. Consider the following way that I use these numbers for in-person purchases.

When I am at the veterinary clinic under an alias name, I am required to pay via debit or credit card due to a cashless system during the COVID-19 pandemic. I advise them that I have a virtual card which I can read to them. I read the number, expiration, and three-digit code aloud to them while they enter it within their sales processing system. The charge completes as with any other card. If someone is listening and tries to use the number at another establishment, the charge will be declined due to the merchant lock. This allows the purchase to be processed under my alias name and any local postal code.

Note that the BILLING address entered into an online payment option is sent to Privacy.com, and it is stored there for seven years per federal law. It is not shared or sold, and is secured internally. Because of this, I always use a random address for billing information, but a true address for shipping details (when required). Since Privacy.com allows any address to be used during checkout, there is no need to ever provide a true billing address which is associated to your home. The exception is for services which require the billing and shipping details to match. For those, I typically ship to a CMRA such as a UPS store or other mail drop.

Privacy.com Concerns

It would be false to say this service was a perfect privacy solution. Any financial institution is bound by government requirements to track and verify users, and Privacy.com is not immune to these demands. This service relies on a third-party company called Plaid in order to verify user identities. We do not know the depth of involvement Plaid has with Privacy.com, but we know there is an exclusive relationship between the two. Since Plaid connects to thousands of banks and is primarily funded by companies such as Goldman Sachs, American Express, and Citibank, I had assumed that various levels of data sharing existed. This is not a pleasant thought, but the best option we have for free virtual debit cards.

In 2021, Plaid created an online sharing portal at my.plaid.com with the goal of providing individuals information stored from within their financial accounts. I never recommend this type of activity. You are required to connect your bank and Privacy.com account to Plaid's servers. Instead, consider visiting <https://plaid.com/legal/data-protection-request-form/> and requesting a copy of all available data stored about you by Plaid. After receiving the information, you can request removal of all data within this same page if desired. I completed all processes and discovered that Plaid possessed absolutely no data about my five years of Privacy.com usage, and no details from the shipping addresses used during online orders. This was quite a relief and calmed my fears about the relationship between the two companies, which exists solely for account verification.

What does this mean in the real world? I believe that transactions through Privacy.com provide value to us. They allow us to use alias names and prevent merchants from knowing our true identity and account details. It helps us prevent credit card fraud and unauthorized card transactions. It is NOT a mechanism to hide transactions from banks, governments, or credit agencies. I believe the anonymization protections stop immediately after the merchant. It is important to understand these limitations and not assume this service is a magic solution. While I rely on Privacy.com card numbers every day on behalf of myself and clients, it can never replace the anonymity provided by cash. I provide the following advice to clients using Privacy.com.

- Never associate your true home address with billing details.
- Always use an apartment address in another state as the billing address.
- Never fund a NEW online shopping account with a Privacy.com card.
- Attach Privacy.com cards to established online accounts with purchase history.
- Delete cards which will no longer be used.
- Pause cards which are not currently being used.
- Activate “Private Payments” within the service.

Trust / LLC Checks

If you established bank accounts in the name of your trust or LLC, you may wish to have checks available for semi-private payments. If you need to write a check for a product or service, one from a trust account without your name may provide more privacy than a personal check containing your name and address. When you open the bank account, most institutions will give you some free temporary checks. These are designed to provide immediate payment options while you wait for a full order of checks to arrive. If you decide to go this route, please consider the following.

The bank will usually offer five to ten free checks. They print them on-site on professional paper stock. I like these because they are usually the larger sized version which appear more professional than a smaller personal check. I always push the limits here and ask for double the amount offered. On one occasion, I encountered a new employee who was instructed to do anything to make the customer happy. I walked out with 150 “temporary” free checks. These checks do not expire, and you may never need to order more.

The bank will likely place all known details on the checks. This often includes the LLC or trust name, your name, your address, and your role in the entity. This eliminates any sense of privacy. I always ask that only the name of the trust or LLC appear on the check. If questioned, I advise that I might be moving soon and would rather not provide an inaccurate address. Most importantly, I do not want my name listed on the check. Most banks comply with this request.

If you need additional checks, I do not recommend ordering through your bank or any third-party services. Regardless of your directions to the bank, it will still likely place your name and address on the checks. Third-party check printing services are more demanding. Due to fraud and abuse, most now require you to include a name and physical address which can be verified through public records. They will only send the checks to the address printed on them.

I prefer to print my own checks. This may seem shady, but it is completely legal. I purchase professional check paper through Amazon and create an Excel spreadsheet for easy printing. I can now print my trust name with routing and account numbers at the same time I enter details about the payee on the check. I can choose whether to include any address I like, such as my PMB or UPS box. Usually, I do not include any address. Printing your own checks allows you the freedom to control the data disclosed within each. As long as you are providing accurate entity titles and account details, there is no fraud here. Overall, I possess checking accounts for most of my trusts and a few of my LLCs. I will later specify the few instances when this format of payment is preferred over other options.

Secondary Credit Cards

Most credit card companies will issue additional cards at your request. These cards usually possess the same account number as the primary card and all charges will be applied to the primary account holder. These cards are often requested by parents to give to their children for emergencies or by individuals to allow usage by a spouse. Any time the secondary card is used, the charge is processed as if the original card had made the purchase. Since the secondary card is part of an account that has already been confirmed, there is usually no verification process to obtain the additional cards.

To request an additional card, which you should refer to as “Secondary” or “Authorized User” cards, you should contact the credit card company by calling the telephone number on the back of the card. Tell them that you want a duplicate card in the name of a family member. You can request an additional card in any name that you want, including your new alias. You will be warned by the credit company that you are responsible for any charges, and the new card will be sent out immediately to the address on file for the account. If you do not want this new name associated with your home address, be sure to update your address on file with the credit company to your PMB or UPS box as previously explained. I recommend confirming that the new address is active before ordering additional cards.

Many readers of previous books reported difficulty in obtaining a secondary card from traditional banks, such as Bank of America or US Bank. Readers report that these entities demand a DOB and SSN for each secondary card holder. I have found this technique to work best with traditional credit card companies, and it has never worked for me with a debit card. In a moment, I present my updated recommendation for secondary cards since the previous edition of this book.

You may be reading this and thinking that there is no way that this could be legal. It is absolutely legal as long as you are not using this method to commit fraud. The card is attached to your account, and you are paying the bill. It is not identity theft because you are not claiming to be a specific person. If you were using someone else’s Social Security Number and opening credit lines with their information, then this would be illegal. You must only apply this to your own account over which you have authority. Additionally, you must always follow the rules.

- Never provide your alternative name to law enforcement or government officials.
- Never open new credit lines with your alternative name.
- Never generate any income with your alternative name.
- Never associate any Social Security Number with your alternative name.
- Never receive any government or community benefits in your alternative name.
- Only use this name to protect your privacy in scenarios with a credit card.

Secondary Credit Card Concerns

There is a fine line between the use of an isolated alias name and possessing a secondary credit card in that name. If an alias name is needed due to death threats, you should never obtain a secondary card in this new name. This is because the credit card company associates you to the alias and reports this information to numerous third-party organizations. Consider the following scenario which represents my own unfortunate experience with Chase.

I possessed a Chase credit card in my true name, associated with my SSN. During the application process, I requested a secondary card in an alias name. For my own privacy, I will not disclose the name. Assume it was "Mike Doe". I never used the card which was issued in my true name. I only wanted the account for the secondary card in my travel alias name. This way, I had a credit card in an alias name when I checked into hotels under that alias. Since I had never used that card in my true name, I should have some isolation between me and my alias. This is actually quite incorrect.

A few months after I began using the secondary card, I conducted a query of my own name within the data aggregation service CLEAR. My report immediately identified "Mike Doe" as one of my associates and aliases. This is because Chase shares the details of every card holder with dozens of other companies. Per their online privacy policy, Chase shares full details of your account and transactions for "joint marketing with other financial companies" and their "affiliates' everyday business purposes". In other words, Chase tells others what you are doing. Furthermore, Chase does not allow you to limit or prohibit this sharing. While all credit cards share some data about your transactions, Chase seems to go overboard. Because of this, I have canceled all of my Chase cards and I no longer recommend them to clients. In a moment, I explain my current process.

Secondary cards have caused much confusion with my clients. I present two scenarios which may help identify when it is appropriate to use a secondary card and when it should be avoided.

- I possess an alias name which I use while I travel. I check into hotels under this name and I possess a secondary credit card in the name. It is loosely associated to me through financial records, but not within public people search websites. It allows me some privacy while outside my home but a non-public digital trail exists.
- I possess an alias name which is extremely confidential. It is only used in situations where I do not want to be associated with my true identity. It has been used during the purchase of my VPN, cellular telephone, and mobile data plan. I would never obtain a secondary card in this name. It would create a trail from me to the services and devices for which I want to remain private.

Current Secondary Credit Card Protocol

I have possessed secondary credit cards in various alias names for over a decade, and I have helped countless clients replicate their own process. In 2020, I substantially changed my credit card protocol for clients. As stated previously, I no longer recommend Chase cards, and now encourage clients to obtain American Express (AMEX) accounts. Part of this is because all Chase transactions are captured by both Visa and Chase, and both refuse to allow you to control sharing of the data. Chase's online privacy policy also clearly boasts that you cannot limit data sharing to third parties. Let's compare that to American Express.

If you log in to an active AMEX account and navigate to Account Services > Security & Privacy > Privacy Preferences, you will see similar third-party sharing options which were present with Chase. However, AMEX allows you to disable all of them, which I recommend doing. In fact, AMEX was the only card I could find which allowed the consumer to prohibit sharing to outside companies. Furthermore, since AMEX is not affiliated with Visa or MasterCard, you are eliminating additional exposure by keeping these purchases within the AMEX network. However, there is one more area to adjust. Navigate to the following direct website and disable "Information Sharing" on any card presented.

https://online.americanexpress.com/occ/auth_inquirepiisharing.do

After these modifications, I believe you possess the most private credit card option available today. No credit or debit card is anonymous, and all leave a digital payment trail. Since daily credit card use is required by most of my clients, I simply try to find the lesser of all evils.

AMEX encourages additional authorized user cards for both personal and business accounts. You can submit a request online or via telephone. However, AMEX demands an SSN and DOB be attached to every secondary credit card issued. This presents a big problem if you want a card for "John Doe" but do not have a valid SSN to provide which matches that name. Instead, consider a new strategy. For most clients, a secondary card with only their first and middle names works fairly well as an alias. Assume your full name is George Michael Bluth. Using George Bluth, Michael Bluth, or the full name could be a privacy invasion, especially when checking into a hotel. However, George Michael is generic. It is also not a lie. Many clients have expressed concerns about using a completely fake alias, especially those carrying security clearances. Using only a first and middle name is usually much more acceptable.

I typically tell a client to call AMEX and ask for a secondary card be issued in only the first and middle name. Explain that you are the victim of stalking, and prefer not to use your last name at hotels. Advise the AMEX personnel to add your own SSN to this card. The new card will not have your last name displayed. I believe there is a much clearer legal use of an alias card which displays true information than one which is completely fake.

For extreme clients, I still rely on completely alias-named cards through AMEX business accounts. Although AMEX encourages users to add an SSN and DOB for each cardholder, the business accounts allow more discretion, and they will issue cards to any name desired without providing an SSN when pushed. Recently, the following steps were used with a client.

- Generate an EIN from the IRS for your LLC. If you do not have an LLC, register for an EIN as a sole proprietor. AMEX may scrutinize sole proprietors for business cards.
- Apply for a free AMEX business card with true name, SSN, and EIN via telephone. During the process, request a secondary card for an employee. When prompted for a DOB and SSN, consider a response similar to, “Our company privacy policy prohibits distribution of employees’ SSNs. I accept all responsibility for the usage of the card and authorize my own SSN to be used.”
- Provide one or multiple alias names for the new “employee cards”.

I have helped clients obtain business cards as sole proprietors without the need for an LLC on numerous occasions, but having an LLC EIN provides a much smoother process. One client possesses a business account with over 20 alias cards without ever providing any additional SSNs. The limit imposed by AMEX is 99 cards, but I never recommend testing this. Finally, I present what I believe is the best feature of the AMEX secondary business cards: each card possesses a unique number. While the numbers are very similar, the last five digits are unique. Consider the following reasons why this is important.

- A retail business does not know that your alias card is under the same account as your personal name. If you had used your real Chase credit card at a grocery store and later switched to using the alias Chase card, the store knows the same number is on each and treats the purchase history as one. AMEX cards are not vulnerable to this.
- Many online retailers restrict credit card numbers to a single account. If you have a credit card number within an account in your true name, creating an alias account with the same number will cause issues.
- Companies which share purchase information with third parties will not be able to disclose that your personal card number is associated with your alias card.
- Hotels cannot associate your previous true name with your new alias by comparing credit card numbers used during payment.

AMEX is far from perfect. It is still a credit card company profiting from your activity. Compared to traditional Visa and MasterCard providers, I believe AMEX is a much better choice for both privacy and alias usage. Be aware that AMEX conducts a soft pull on your credit each time you request a secondary card, and will require a credit freeze to be lifted each time you add a card. I always recommend applying for any desired secondary cards at the time of application in order to avoid these roadblocks.

Alternative Secondary Credit Card Protocol

There are three concerns from some clients in regard to AMEX credit cards. The first is that AMEX typically requires a slightly higher credit score than most Visa providers in order to be approved for an account. The second is the occasional merchant which does not accept anything other than Visa or MasterCard. Finally, some clients do not want the awkward telephone call with AMEX support during which they must convince the representative to create a secondary card in one name while associated to the SSN of the account holder. Most clients want a simple option for numerous secondary alias credit cards without much resistance from the provider. In these scenarios, I recommend Capital One credit cards.

First, I should note that Capital One has a privacy policy almost identical to Chase. You cannot control the major data-sharing abuses. If you choose a traditional credit card such as these, I believe it is vital to be using a PMB or other CMRA address as the physical “home” address. They will absolutely share account details with data mining companies and credit bureaus. I do not possess a Capital One card, but I recently helped a client obtain an alias card via a brief phone call. After calling the number on the back of the primary card, we explained that we wished to obtain two “Authorized User” cards, per the following wording on Capital One’s website.

“An authorized user is someone you add to your account without any additional application or credit check. They’ll get a card with their name on it and share your line of credit. As the primary cardholder, you’ll still be responsible for all charges and, if you have a rewards card, you’ll earn on every dollar they spend.”

The representative only asked for the names desired on the cards. After reading a warning about the primary card holder being responsible for all purchases, the cards were shipped. In three days, my client possessed two credit cards in alias names ready for use. Both cards displayed the exact same card numbers as the primary card in her real name. This is a minor issue, but we should all be aware of the risks when using multiple names with the same card number. If the primary card in the real name is never used, this is not much of an issue.

Obtaining secondary cards through Capital One was much easier than AMEX. However, privacy is not always easy. I believe it is worth the effort to secure AMEX cards in alias names with unique card numbers. This helps hide your true identity from merchants. If AMEX is not an ideal option for you, I prefer alias Capital One cards over any card in a true name. You must choose the level of privacy (and effort) desired and then execute your strategy. Expect failure at some point, and then keep pushing until you achieve the level appropriate for your needs.

Secured Credit Cards

I have not found a credit card provider which would agree to provide an alias card in the name of only a trust or LLC. This is unfortunate as such a card would not include any name at all, eliminating the need to use an alias. Traditional business credit cards require your SSN and a full credit check, and they will still place your name on the card above the trust or LLC name. My only solution to this is to obtain a secured business credit card. Secured business cards allow business owners to set their own spending limits by placing a refundable security deposit that doubles as their credit line. The security deposit is important because it protects issuers from the possibility of default which thereby allows you to qualify for most secured business credit cards regardless of your credit history or how much disposable income you have. For our purposes, a secured credit card replicates a prepaid card, but has a much more professional appearance.

These cards can display a business name, including a trust or LLC, without the need for a real name underneath. There are two main types of secured cards. The first, and most popular is the type that builds a line of credit for the business while it is used. We do not need that. Instead, I search for cards that simply provide a limit equal to the current balance of the account. I also look for cards that do not require an SSN. These will demand an EIN for your business, so these will be limited to LLCs only. If you want a card issued in the name of your trust, you will need to contact numerous companies. Be prepared to be declined, but I occasionally find a new secured card that is less restrictive. The following online searches may be of great benefit.

secured credit card no ssn
secured credit card no ein
secured credit card ein only

Recently, I have found a few physical banks which offer secured business credit cards. If you have already established a personal account at an institution that offers these, it will be much easier to customize your card. I recently entered a bank branch where I possess a personal checking account. I advised that I had created a new LLC, and wanted to obtain a secured credit card. I stated I was not looking to establish credit, and only wanted the card for convenience. I deposited \$1,000 into a new account and received a card with only my LLC name visible within a week. I can now use this card without disclosing my name.

Now that we have your sources of payment established, we need strategies on the proper use of each. There will be many times over the first few months of residency in a new home when a service or utility needs to be activated. You will be asked for your full legal name, address, DOB, SSN, and other sensitive information. None of your personal details should ever be associated with your home address. We will need to be creative and resourceful.

Alias Wallets

Isolating your aliases within their own wallets is vital for my clients. You do not want to keep secondary credit cards in alias names in the same location. Presenting a credit card in one name while you are holding two additional cards in other names looks suspicious. You want to be able to immediately access any credit cards or non-government identification cards as if it were natural. While I can offer a couple of ideas, you should ultimately choose the method best for you. Hopefully the following will generate your own thoughts.

One of my clients carries four “slim” card wallets. These are small, thin wallets which hold a couple of cards on each side with a thin pocket in the middle for cash. He chose RFID-blocking wallets, which is also my preference. These are abundant on Amazon, but I currently only use the Silent Pocket options (amzn.to/3tmB7kl). These are available in several colors, and the following is the strategy he and I found best for his needs.

- **Blue:** This wallet is associated with his true identity containing his real driver’s license, passport card (no address) and credit cards. He chose blue for this one as it is the wallet he will retrieve when stopped by the police for his awful driving (blue lights). The passport card can be used when an official ID is needed, but he does not want to share a home address (PMB).
- **Black:** This wallet is his primary alias that he uses for travel purposes. This contains a secondary credit card in his alias name which he uses for hotels, dining, and social interactions. It also contains his alias gym membership card, “employer” ID, and random travel reward cards. They are all in the primary alias name.
- **Green:** This wallet is designated only for shopping (green reminds him of money). It possesses prepaid credit cards and gift cards. No identification is required. He grabs this whenever he will be purchasing anything from a physical store.
- **Red:** The final wallet is red and only used during international travel. It is the larger style of passport wallet. It contains his passport, official state ID in his real name, and a second credit card in his real name reserved for international use. It is the primary form of payment for this wallet. Each of these four wallets contain a few hundred dollars in cash for emergencies.

Another client chooses to use binder clips as his wallets. His situation is very unique and he possesses four “wallets” at all times. Each set contains the appropriate identification cards and secondary credit cards, with a small amount of cash folded once around the cards. The small binder clip holds it all together. He knows immediately which alias is represented by the type of currency on the outer layer of the wallet. The \$20 bill is the primary, the \$10 bill is the secondary, the \$5 bill surrounds the third alias option, and a \$2 bill covers the fourth.

ID Scanning and Copying

A previous chapter briefly discussed optional responses when a car dealership demands to copy your license when purchasing a vehicle. I want to revisit this under new context. We now see many retail establishments demanding to store scanned copies of identification or collect text details of IDs from various barcodes stored on the backs. This is usually unnecessary and the data collected is often abused. I have witnessed the following scenarios within one month while updating this chapter.

Retail Returns: Due to an abundance of gift card fraud, retail establishments have cracked down of returns of products. Stores such as Walmart and Target are members of an entity called Retail Equation. This company monitors returns to retail stores. When the store requires identification in order to return a product, they typically scan the ID card and the details are sent to Retail Equation. If your passport card does not populate the desired fields, the employee will likely manually enter your details. All of your returns are stored and analyzed. If you return enough products to trigger a flag on your account, stores will stop accepting returned items. Your profile is available to many companies and other unknown recipients.

Medical Organizations: Any visit to a doctor, dentist, hospital, or urgent care is going to require identification. I accept this, as they need to verify insurance benefits and ensure proper prescription details are transmitted. However, I do not allow anyone to collect a digital scan of my photo within any identification card.

Pharmacies: I recently required a prescription eye drop. It was not a controlled substance, and not a medication which is abused. However, the pharmacy demanded I present valid ID. After displaying my passport card through a windowed wallet, they demanded I remove the card so they could scan it into their system. The scan was a digital acquisition which would populate my details and store my photo forever across their nationwide network. No thanks.

Entertainment Establishments: In late 2019, I went out with friends to a comedy show in Los Angeles. After submitting my ticket for entry and displaying my passport card to prove I was of legal drinking age, I was told they needed to scan my ID into their system. When I asked where the data was stored, the level of encryption applied to the transmission, and to see a copy of the terms of service for this requirement, I was told to move along.

Adult Products: If you have ever purchased alcohol, you have likely been “carded”. Many years ago, this meant flashing my ID and the clerk doing the math to make sure I was of age. Today, stores require the clerk to scan the barcode on the back in order for their systems to determine that my date of birth is valid for purchase. Many of these systems record the details and share them with third parties.

My solution to this is two-fold. First, I only provide a U.S. passport card whenever an entity wants to scan a barcode stored within an identification card, such as a grocery store. This is because the barcode on the back of a passport card simply contains the numeric digits directly to the right of it, which only identifies your card number. There are no personal details stored within this code. Furthermore, most businesses, such as grocery stores, do not have software which knows what to do with these details. The card number obtained during the scan will likely get rejected. Most scanning systems are looking for a date of birth, name, and address. All of these details are present within the barcode of most driver's licenses or state identification cards. Second, I rely heavily on the federal law mentioned earlier. U.S. Code, Title 18, Part I, Chapter 33, Section 701 states the following.

"Whoever manufactures, sells, or possesses any badge, identification card, or other insignia, of the design prescribed by the head of any department or agency of the United States for use by any officer or employee thereof, or any colorable imitation thereof, or photographs, prints, or in any other manner makes or executes any engraving, photograph, print, or impression in the likeness of any such badge, identification card, or other insignia, or any colorable imitation thereof, except as authorized under regulations made pursuant to law, shall be fined under this title or imprisoned not more than six months, or both."

This law was created for military identification cards and insignias, and was likely never intended for our use. I have this exact wording, followed by a URL which can be used to verify the content (<https://www.law.cornell.edu/uscode/text/18/701>), printed onto a sticker and affixed to the back page of my passport. When I use my passport as identification during one of the previous scenarios, such as a visit to a doctor, and an employee insists on copying the identification page, I present this section of my passport. I explain that I could be committing a crime allowing the passport to be photocopied. If needed, I sell it further by telling the employee that he or she may definitely be committing a crime by doing so. It is always met with skepticism, but most employees do not want to take a chance with federal law. I always offer them the URL so that their manager can look up the law and see if they agree. Most do not indulge me, and move on to the next requirement of my visit.

Whenever you make purchases using the techniques throughout this book, you are likely to be asked for identification. I hope that you consider these solutions when this happens. I have encountered numerous data breaches which included full digital scans of passports and identification cards. I do not want to ever be exposed within these common occurrences, and I suspect you feel the same way. The more of us who refuse this unnecessary privacy invasion, the more common our rebelliousness becomes. It may create awareness for future visits. When all else fails, and an employee demands to copy my ID, I respond "Of course! However, I would like a copy of yours first. Is that acceptable by you? If not, why?". I have yet to experience an employee allowing me to copy their ID, as that would be a privacy invasion.

Home Insurance

Acquisition of any type of insurance always brings difficulties when attempting to achieve privacy. Insurance companies want to know whom they are protecting. They will use your credit score to determine their risk providing you coverage. Misrepresenting yourself or your entity is not only illegal, it will likely eliminate any payout when you need to file a claim. Imagine you provided an alias name to the insurance provider and your home was destroyed. You file a claim, which is approved. The check is written to your alias. How would you deposit it? What if you are required to display identification to receive the check? What happens when a neighbor sues you because of a fall on your property? Your insurance company will not cover you if your name is not on the policy. These are real issues.

The bottom line here is that your home insurance policy will need to be accurate. This does not mean that you must give up all personal privacy. You have a few strategies at your disposal which can provide various layers of privacy while remaining legal and properly protected. Before I discuss my recommendations, I present past experiences that should be avoided.

In 2018, I assisted with the purchase of an estate. My client wanted to remain completely anonymous and was quite wealthy. The purchase of the estate with cash was simple, and the utilities were all activated with alias names or details of the trust. The last issue was insurance. All providers in that area demanded to know the name, DOB, and SSN of the home owner and account holder. The trust could be named as a secondary insured party, but the policy mandated full details of the owner. The insurance companies confirmed that any payment made due to a claim would be paid to this name, and not the trust. There was no budging. Either my client disclosed his true identity, or there would be no policy.

My client chose the latter. He decided to simply avoid home insurance altogether. He was wealthy, could have purchased numerous additional homes in cash, and decided that his privacy was worth more than the money he could lose after a catastrophic event. I discouraged him from this, but his mind was made up. To this day, he possesses no home insurance coverage.

I disagree with this decision for two reasons. First, a home is likely our biggest asset. If a tornado or fire destroys the home of my clients, they are unable to purchase another. If they possess a loan on the home, insurance is mandatory. Economically, it does not make sense to proceed without insurance. Additionally, you now possess great personal liability. If someone is injured on your property, you are the sole party reliable for payment. This could quickly bankrupt you. Therefore, I insist on insurance for my home, and I strongly encourage my clients to do the same.

Some may wonder why we can't use our trustee for the insurance policy. We could, but this is probably a very bad idea. Your trustee would need to provide their own personal details, and the policy would be priced based on their credit history. Next, this would likely violate the terms of the policy. Almost every home insurance policy states that the listed party must be an occupant of the house. The fine print will usually specify that immediate relatives also possess coverage. Technically, you might be covered if your sibling was your trustee, but I think you are playing with fire.

The following methods assume that you established a private home titled to the name of your trust. Whether you possess a loan or paid in cash will not matter. These tactics attempt to obtain completely legal and appropriate coverage for your home.

My first recommendation is a personal visit to a handful of local providers in the area of your home. Calling random online providers will get you nowhere. They will not provide a quote or any details without the immediate demand for your name, DOB, and SSN. These are all out for me. I call ahead and ask to arrange a meeting to speak directly to the local insurance agent for each business. I ask to reserve the meeting under the name of the trust. If I am pushed for a real name, I advise that I am not sure which trustee will be at the meeting. I show up in person, well dressed and polite.

I start with some honesty. I advise the agent that I represent a trust which is in the process of purchasing a home. The occupant(s) of this home are very private. They have been the victims of stolen identity, cyber-crimes, and other unfortunate situations. I further explain that the full details of their identity, including DOB and SSN have been publicly exposed. This likely applies to every American citizen. If appropriate, I conclude that one of the occupants has been harassed and threatened, and is in fear of a physical attack. I explain that I am taking every step I can to ensure that their true identities are not publicized on the internet.

At this point, I rarely receive any resistance. I usually see signs of empathy on the face of the person with whom I am speaking, and all of these scenarios seem very common. I proceed to ask some very detailed questions. I already know the answers, but I find that allowing the agent to discuss the situation creates a better dialogue.

- What information will you need about the owner of the home?
- Can the policy be placed in the name of the trust?
- If not, can the trust be listed as a secondary insured?
- Does your parent insurance company share customer data with any third parties?

In almost every discussion I have had in these scenarios, I learn the following:

- Almost every insurance provider allows the inclusion of the trust name as a secondary insured party, but rarely as the primary policy entity. This applies to traditional home policies. A Social Security Number will be required to generate a new policy.
- Insurance companies insist they never share customer details with third parties. Minimal online investigation reveals this to be inaccurate. As only one example, consider the privacy policy of State Farm. It begins with “We do not sell customer information”. The excerpts below identify the ways in which they share customer details. The content in parentheses is my own opinion of how this could expose your home address.

“We share customer information inside or outside our family of companies”:

- for our everyday business purposes, for public policy purposes, and as permitted or required by law. (This is a catch-all, and gives them the right to do practically anything they desire with your information.)
- as needed, to handle your claim. For example, we may share name, address, and coverage information with an auto body shop to speed up repairs on auto damage claims. (This allows them to share your true name and address with any service provider. This eliminates the idea of using an alias name for the company that will replace your porch after a storm.)
- with consumer reporting agencies, for example, during the underwriting process. (This is the most invasive. These agencies devour your personal information, and amend your profile. You will not be anonymous very long.)
- in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of our business or operating unit. (If this insurance provider is sold to another company, your information is transferred and the new privacy policy applies.)
- with companies that perform marketing or other services for us or with whom we have joint marketing agreements. These agreements allow us to provide a broader selection of insurance and financial products to you. (This basically allows the insurance company to share your details with any company willing to purchase it.)

The summary here is that every major insurance company has the right to do whatever they want with your information and it will be exposed at some point. Therefore, we must take our own precautions. Now that you know the risks, let's establish our best defense possible.

In 2017, I assisted a client with the purchase of an anonymous home. She was the victim of a targeted home invasion, and sought a safe place where she could not easily be found. Home insurance should be secured before the closing date, as you should have protection the

moment you own the property. I visited a major insurance chain that possessed a local office and an independent agent. We made it through the small talk and I explained the unique scenario of my client. He seemed very willing to assist any way he could.

My first concern was the issue with the trust. I explained that my client, and the true occupant of the home, was not the trustee of the trust which is purchasing the property. Therefore, lumping together the entire policy into one entity might not make the most sense. I asked if he could provide a business policy in the name of the trust and a separate renter's policy in the name of my client. This is common with rental homes and other situations where a business entity owns the property but does not reside in it.

With a traditional home insurance policy, there is coverage of the dwelling, property, and liability. There is also protection for the contents. This is a typical "package deal". If you owned a rental property, you would want protection if the house was destroyed or someone was hurt. However, you would have no interest in coverage for personal items, such as the renter's furniture. These policies are more affordable because they provide less protection than a traditional policy. If your tenant wanted coverage, he or she could purchase a renter's policy to cover only their belongings. I like to apply the best of both worlds toward my clients' policies.

I explained that I desired a policy in the name of the trust as a business entity for the home and property. The trust obviously will not be an occupant. The trust would own the policy and make payments. The trust is covered from a liability perspective and the property is covered from damages. This type of policy is commonly used for businesses. Since no business will be conducted, and the property is not open to the public, the fees associated with this type of policy are usually quite affordable.

For my client, I requested a renter's policy in her name. This covers her possessions inside the home. One way to explain it is that the policy would cover anything which fell out of the house if you were to pick it up and shake it. The business policy protects everything else including liability. These policies are very affordable, as there is a much less likely risk of a claim.

The reason I want to do this is because it allows me to have the home policy purely in the name of the trust. While the renter's policy will be in the name of my client, I have a bit more control over the information stored in that account. The provider will obviously know that my client lives in this home. However, I can place the address of a UPS box as the primary contact for the renter's policy. If the details of this policy are shared, sold, or lost, the associated address will likely be the UPS box. While a business account can also possess a UPS box for billing, there are many references to the real property address all throughout the policy.

You may recall that I previously wrote that an SSN must be associated with the policy. This is absolutely true. Since I am purchasing the renter's policy through this office, and supplying a full name, DOB, and SSN of my client, the office now knows the true identity. The "soft pull" credit check for the renter's policy can be used to pacify the requirements for the trust policy. As the grantor of the trust, my client has a direct nexus, even if she is not the trustee.

As an extra layer of privacy, I proposed an additional request. I explained that my client is considering returning to her maiden name. I requested that the renter's policy be placed into this maiden name now, even though it is associated with her true DOB and SSN. The company will know her true name through the credit check, but the policy and annual bill will be in the maiden name. This isn't going to fool an advanced private investigator, but it will make her a bit more difficult to find in the wake of a large data breach. Let's summarize the coverage.

My client possesses a trust. She is the grantor but not the trustee. The property is protected with a business policy in the name of the trust. It covers the home, land, and liability of both. My client's name is not listed anywhere in this policy, and the trustee digitally signs the official policy, executing it at the time of closing. This annual bill is paid with a designated Privacy.com debit card, which is connected to the trust's checking account.

My client possesses a separate renter's policy which is in her real maiden name and SSN. It covers her belongings inside the home. The address for the policy and billing is her UPS box. The policy contents include the real address, which is not public record. This bill is automatically paid through a second Privacy.com debit card, connected to her personal checking account.

Is this bullet-proof? Not at all. The insurance company is the weak link. They know my client and her home address. This is not optimal, but is the closest we can get to our desired level of privacy. Two years after I executed this plan for my client, I am still unable to locate any official connection between her name and the address of her home. This is the best I can do for her situation. The irony of this scenario is that the combined cost of her trust policy and the renter's coverage is less than the policy quoted as a traditional full coverage home. The business policy even has twice the liability protection. This is mind boggling.

If you do not possess a Privacy.com account, a personal credit card could pay the renter's policy and a check in the name of the trust could pay the home coverage. The formalities of this are not too important, but I like to pay with separate accounts when possible. Your mileage will vary with this. I have presented this proposal to over thirty insurance companies in various states. My success rate is 45%. With enough determination, you can achieve your own success. I insist you be honest with the person with whom you are speaking. A policy is useless if you can't file a claim due to inaccuracies within the application. Allow the local agent to make the policy work for your situation.

Utilities

The next hassle is dealing with the power and natural gas companies. Thanks to fraudsters that rack up large bills and then leave town, you and I must now provide access to our credit profiles in order to establish basic services. The default demands of these companies are to obtain a full name, DOB and SSN. This information will be verified with a consumer agency and attached to your profile. These services will then share this data with additional data mining companies. It is a vicious cycle.

Over the past five years, I have had various levels of success using alias names and sob stories. Many of these techniques no longer work. If I claim I am not an American citizen with an SSN, I am required to send a photocopy of a passport. When I state I am the victim of identity theft, there is no longer any sympathy. When I offer to provide a deposit for services in lieu of an SSN and credit check, I am told this is no longer an option, and I may be required to provide a deposit regardless. With these rules in place, we must be more creative.

Similar to home insurance, I always establish utilities in advance of closing. You never want to be in a rush to turn on the power. You may give in and disclose your real information just to get past the process. I always start with a polite call to the utility company. Since I record all of these conversations (when legal within one-party states), I can provide an exact transcript of a recent attempt for a client.

"Hi. I have a closing date approaching for a home in [CITY]. The property is being purchased by an established trust, and there are not any occupants defined at this point. What are your options for establishing power in the name of a trust?"

This resulted in the expected response. The operator insisted that a DOB and SSN of the resident would need to be provided. If the trust is a registered business with an EIN, this will usually suffice instead of the SSN. None of these situations apply to us, so I continued with the following conversation.

"I see, thank you. I don't know the SSNs of the eventual occupants, and I don't believe the trust has an EIN due to tax filing requirements. The last property we purchased allowed us to place the bill into the trust name as long as we offered either a deposit or enrolled in autopay from a checking account in the name of the trust. Are these possibilities?"

This resulted in a hold time of five minutes while she contacted a supervisor. I had to eventually talk with this supervisor the next day, but it was a productive conversation. The supervisor confirmed that the utility can be opened in the name of the trust with several requirements. The power company would create an account for the trust the day of the call, but services would not be scheduled. The utility profile would need a checking account

attached to it, and it must be enrolled in auto-pay. The checking account must be in the name of the trust. A debit card was not enough. After this was complete, the supervisor could manually approve the account after a scheduled small test withdrawal from the account. After this, a date could be provided to switch on the utilities.

I completed all of these requirements without any issue. The supervisor was very kind about the situation, and more relaxed after she could see the checking account within the system. Every month, the bill is paid through this account. The power company does not know the name of my client. They receive their owed fees in a timely matter every month. There is no fraud. They know the generic name of the trust, which will also be on public record as the owner of this property. The trust checking account is not associated with any personal bank accounts. The bank knows that a monthly bill is paid to a specific utility, but does not know the exact address. The bank knows the identity of my client.

There is an obvious financial trail which could be followed with the proper court orders required. Without these court documents, the name and address of my client will not be connected. You should identify your own threat model, and ensure that you choose the most appropriate tactics. The alternative to this, if you do not have a checking account associated with the trust, is to attempt the use of auto-pay to a Privacy.com debit card. I always offer to pay a deposit to set them at ease, which is usually not required.

Paying a large upfront deposit, which is usually the average monthly bill for three months, will often eliminate the requirement of a credit check. The success rate of this method is decreasing. In a recent worst-case scenario, the utility offered to bypass the credit check only if I submitted a deposit of an average year of use. My client had to give them over \$2500 in order to stay private. I have had much better success by using a checking account in the name of the trust. I encourage you to identify all of your options before choosing the best route.

Once you have power established, the rest is easy. Often, the water and sewer companies will rely on your registration with the power company to confirm service. I usually recommend establishing auto-pay to a Privacy.com debit card. If there are fees associated with this, or you do not have that option, auto-pay to a checking account in the trust name should pacify their demands.

Overall, I prefer to establish all services in the name of the trust. Since some utilities are loosely connected to the city government, use of false aliases could approach criminal behavior. With a proper trust in place, you might not need any aliases. When electronic documents require signing, your trustee has the legal authority to comply. When these companies release your billing details privately and publicly, there will be minimal damage. The trust is already publicly connected to the property.

Internet Service

I believe that the most important utility or service which you can anonymize is your home internet connection. Possessing internet service at your home address in your real name jeopardizes your privacy on multiple levels. Many providers use their subscriber list for marketing and it often ends up in the hands of other companies. This will eventually make your home address public on the internet as associated with you. This is possible with any utility or service that is attached to your home address. However, your home internet account shares another layer of your life that you may not realize.

Internet service providers (ISPs) create the connection required for you to have internet access. In its simplest terms, a cable or phone company possesses a very large connection to the entire internet. It creates its own connections to its customers (you). This might be in the form of a cable modem connected to the main connection coming into your house. This allows you to connect to the entire internet through them. Therefore, the ISP can monitor your online activity. Other chapters explain how to mask this traffic with virtual private networks (VPNs) and other technologies. However, you cannot stop the ISP from seeing the amount of traffic that you are sending and receiving, the times of the day that you are online, and details of the devices which you are connecting to their system.

Those who use the technologies previously discussed in this book will likely be protected from the invasive habits of ISPs. However, people make mistakes. You might forget to enable your VPN or it might fail due to a software crash. You might have guests who use your internet without practicing secure browsing habits. Consider the following scenario.

Every day, numerous people receive a dreaded letter from their internet service provider. It states that on a specific date and time, your internet connection was used to download copyrighted digital material. This is usually in the form of movies or music. This practice usually occurs when law firms monitor data such as torrent files which are commonly used to share pirated media. They identify the IP address used for the download, contact the provider of the IP address, and demand to know the subscriber information. The providers often cooperate and share your details. You then receive a notice demanding several thousands of dollars in order to avoid a lawsuit. Not paying could, and often will, result in legal proceedings. There are numerous cases of people who have lost the lawsuit and have been ordered to pay much more than the original asking amount.

I am not encouraging the use of the internet to obtain files which you do not have the authority to possess. I also do not advocate fishing expeditions by greedy lawyers looking to take you down. I see another side of the problem. What if someone uses your Wi-Fi to commit these acts? What if malware or a virus conducts activities which are seen as infringing? I believe one solution to this issue is to simply have an anonymous internet connection. These methods will

only work if you have gone to the extent of residing in an anonymous house as previously explained. If you have not, or are not going to that level, it does not hurt to apply these methods for a small layer of protection. The following is a true example from a client.

My client had recently moved into his new invisible home. He was renting, and nothing was associated with his real name. The electricity and water were included in the rent and associated with the landlord's name. However, there was no internet access included with the rent. My client contacted the telephone company to take advantage of a deal for DSL internet service at a promotional rate of \$24.99 per month for two years. He did not need anything faster than this access, and liked the price. He gave an alias name and the real address for the service and was quickly asked for a Social Security Number (SSN), date of birth, and previous address. He tried his best to convince the operator that he would not give this out, and she politely stated that their policy is to conduct a brief credit check before providing access. He gave up and terminated the call. He emailed me asking for guidance. While I had dealt with similar issues for myself and others in the past, it had been a while since I had tested my methods with all of the providers. In exchange for me helping him without any fees, he agreed to share his experiences here.

I first contacted the telephone company offering the DSL connection. Before giving any personal information to the operator, I politely asked about the signup policy and what type of credit check would be conducted. I was told twice that a "soft pull" would be conducted based on the SSN of the customer. This was to ensure that there were no outstanding bills from previous connections and to simply verify the identity of the customer. While telling my sad story of identity thefts, harassment, and threats to my life, I pleaded for a way to obtain service to no avail. Part of the issue here was that a two-year contract was required, and they wanted to be sure that they would get their money. There was nothing to gain here.

I searched for other service providers and found two possibilities: Charter Spectrum cable access and various satellite internet options. Due to speed and cost, I wanted to avoid the satellite option. I contacted Charter and verified the service connection to the residence. They had a high-speed connection of 60 Mbps offered at \$59.99 per month. I assured them that I had never had Charter in the past, and asked if there was an introductory price similar to the DSL offer that I had been quoted. As usual, the representative came up with a lower offer. He acknowledged a new customer offer at \$39.99 (taxes included) per month for up to one year. I accepted that and knew that my client could likely later negotiate that cost down through threats of canceling when the first year was finished.

I provided my client's address, an alias name that had already been established and associated with a secondary credit card, and requested automatic bill pay through the credit card. I was told that I could set up the automatic payment myself after the account had been established. This was even better. If I were to repeat this process today, I would use an alias name and a

Privacy.com card. This gives my client more isolation from his true credit card account. I got to the end thinking things were too smooth when the personal questions arrived. He needed my SSN in order to complete the process.

I had dealt with Charter in the past and was able to bypass this requirement, so I started testing the situation. I first stated "Oh wow, I was not prepared for that. You see, I was recently the victim of identity theft and the police told me I was not allowed to give out my SSN until the investigation was complete". The operator was very sympathetic and placed me on hold briefly. He then asked for a date of birth in order to conduct the query. I continued to resist and stated "I think that would be the same as giving you my SSN. I will give you my credit card right now, can I just auto pay?". I was then greeted with something I did not expect. The operator stated "The system demands at least a year of birth, can you give me that?". I took a moment to evaluate the risk and provided a year of birth which was not accurate. This seemed odd to me because there is not much the operator could do with that limited information. However, it was enough to get to the next screen. He now needed an email address for the account details and monthly electronic billing. It is always important to have this alias email account ready before any calls are made. He finished the order and the call was terminated.

Three days later, Charter arrived at his house and installed the service. They provided a modem, and charged \$29.99 for installation. My client had his secondary credit card ready, but he was never asked for it. Charter conducted the installation, activated the service, and left without collecting any form of payment. The next day he received an email notifying him of a payment due. He created a new account on the Charter website and provided his secondary credit card for the payment (Privacy.com is a better choice today). He then activated automatic payments to that card and enabled the paperless billing option. Today, he continues to receive internet service from Charter and pays his bills automatically through his secondary credit card. Charter does not know his true name. He has committed no fraud. He is a loyal customer and will likely pay Charter for services for the rest of his time at this residence. Charter did not require any contract and he can cancel any time. I was pleasantly surprised.

I thought that this may be a fluke. Maybe I was lucky with that operator. I decided to test the system again. However, this time I would contact all of the providers. I decided to contact each major internet provider through two separate calls and document the results. My goal was to identify the personal information requirements for each provider in order to activate service to a residential home. The following were my findings. Please note that your experiences may differ.

I started with Comcast. I assumed that they would be the worst to deal with. This is probably due to years of negative publicity in reference to horrible customer support. They were actually quite pleasant. I stated on two calls with two different employees that I wanted internet service but would not provide an SSN. The first employee stated that an SSN was required for a "risk

assessment". I inquired on ways to bypass this requirement and discovered that Comcast will eliminate this requirement and risk assessment if the customer pays a \$50 deposit. The deposit would be returned after one year of paid service. The second employee also stated that an SSN was required for a "risk assessment" and that there was no way to bypass this. I mentioned the \$50 deposit, and after a brief hold was told that the deposit would eliminate the requirement. I have had two clients since these conversations who have confirmed that Comcast will provide service to any name supplied as long as a credit card deposit of \$50 was provided. I consider this a fair compromise. Comcast also did not require a contract of any specific length of service.

I contacted many of the most common internet service providers in the United States. I asked a series of very specific questions in order to identify those that would allow an account to be created in an unconfirmed name. The table that follows this section displays my results. The categories of the table are explained below.

SSN Required: If the provider requires a Social Security Number (SSN), they will likely perform a credit check. This will associate your real name with the address of service.

DOB/DL Required: If the provider requires a date of birth or driver's license number, this is also a strong indication that a soft credit check will be conducted. This is likely a risk assessment at the least, and will also attach your name to your home. Using anything but your real full name will result in a denial of new service.

Contract Required: This indicates whether the provider requires you to sign a contract for service. This usually locks you in to a set period of time before you would be allowed to cancel. This is not a concern as far as a commitment to service. However, signing a false name here could get you into trouble in civil court. I discourage using any name aside from your own on any binding contract.

Deposit Required: This field identifies the deposit required in order to bypass the credit check mandated by most companies. Paying this amount, as well as the monthly service fee, ahead of service will often eliminate the requirement of a verification check of your name. I welcome a deposit requirement in lieu of providing personal details.

Credit Check Required: This column identifies the companies that absolutely require a full credit check. I have found no way to bypass this requirement with the providers listed. This will certainly associate your name to your address and will be present through online resources.

Prepaid Option: Only Xfinity Prepaid offered truly anonymous service without a demand for any personal information. This requires an upfront purchase of a modem and "refillable" monthly service. My only complaint is the 20 Mbps download and 1 Mbps upload speed.

Provider	SSN Required	DOB/DL Required	Contract Required	Deposit Required	Credit Check
AT&T	No	Yes	Yes	No	Yes
CenturyLink	No	No	Yes	\$75	No
Charter	No	No	No	No	No
Comcast	No	No	No	\$50	No
Cox	No	No	No	\$40-\$65	No
DishNet	Yes	Yes	Yes	N/A	Yes
Earthlink	No	No	No	Varies	No
Frontier	Yes	Yes	No	N/A	Yes
Verizon	No	Yes	No	No	Yes
XfinityPrepaid	No	No	No	No	No

Your experiences may vary from mine. Overall, most internet service providers stated that an SSN and credit check were required for service at first. When pushed on alternative options, many acknowledged that this information was not required. I found that the following two questions gained the best results when talking with a sales representative. I encourage you to be persistent. Overall, the person you talk to wants to complete the sale.

- I was recently the victim of identity theft and was told to no longer disclose my SSN. Is there any way I can provide a deposit instead of giving you my personal details?
- I reviewed your website offer details and I will be paying automatically by credit card in order to forego giving you my SSN or DOB. Is this still your policy?

Mobile Internet Hotspots

In the past year, I have encountered many clients who struggled to obtain internet service anonymously. Some lived in rural areas with limited options, such as landline DSL. Most of these providers demand a true name, date of birth, SSN, and a soft credit pull. Other clients planned to travel constantly or live out of an RV for a while. In these rare situations, I have had better success with mobile internet hotspots over traditional wired internet connectivity. I have been able to register Verizon, T-Mobile, and AT&T mobile hotspots with pre-paid contactless access without providing any true identity. You will pay more for this luxury than traditional services and be limited on the amount of data. If you choose this option, know that video streaming may be an issue and can deplete your data quickly. I only recommend these when clients accept that email and web browsing is allowed, but large downloads may cause problems. If this is of interest to you, identify the best signals in your area and focus on the carriers with the strongest reception. Always obtain the most data you can afford. If desperate, your GrapheneOS or Apple iOS device can serve as a mobile Wi-Fi hotspot to multiple devices. Make sure you have a data plan which supports this decision.

SSN Alternatives

Whenever a utility service demands an SSN for a client, I often respond that the client is not a U.S. citizen (an actual scenario where this worked for a client is explained later). Sometimes, the utility will demand the equivalent number for that person's country, which is often referred to as a National ID Number. I am always prepared for this. Most utilities will accept practically any number you give them, but some will use an online service to verify the number conforms to the country's standard. Canada uses the Social Insurance Number (SIN) system. The following three SINs will verify as valid, but will never be assigned to anyone.

903 841 278
991 598 558
902 280 171

The United Kingdom uses the National Insurance (NI) number, and the following three NIs will verify as valid, but will never be assigned to anyone.

SX 87 58 64 B
KR 11 23 28 A
RY 61 81 33 D

Mexico uses the CURP system which is an 18-character alphanumeric code. The first digit is from the first letter of the paternal surname; the second is the first internal vowel of the paternal surname; the third is the first letter of the maternal surname; and the fourth is the first letter of the given name. This is followed by the six numbers that are the person's date of birth in YYMMDD format; one letter describing the person's gender ("H" for male and "M" for female); two letters which are the abbreviation for the state where the person was born; the first consonant of the paternal surname; the first internal consonant of the maternal surname; the first internal consonant of the given name; a character to avoid duplicate CURPs; and finally, a character that is a checksum. An example may appear as "BAAQ800201HMNRLF03". However, do not use that number, as it may be associated with a real person.

By simply changing the date of birth to a date prior to 100 years and changing the seventeenth digit to "9", we should be able to avoid intruding on anyone alive or deceased. The following would pass structure validation for a Mexican CURP.

BAAR200201HNERLF93 (Male-Born Abroad)
MAAR200201MNERLF93 (Female-Born Abroad)

Amazon Orders and Issues

I devote an entire section to Amazon for two reasons. First, it is an immensely popular online retail establishment, even with privacy enthusiasts. Second, I encounter constant issues attempting anonymous purchases, as do many readers. I place orders through Amazon weekly and never jeopardize my privacy during the process. If you are already using Amazon and have an account created, I recommend that you stop using that account and create a new one in order to prevent further tracking of your purchases. You may be surprised to learn about the data shared with Amazon sellers, which is explained in a moment. The details which you provide within a new account are very important. Before discussing the appropriate methods, please consider an actual scenario.

A client had moved to a new rental house to escape a dangerous situation. She had nothing associated with her real name at the address. The utilities were still in the name of the landlord. She used a PO Box for her personal mail. She was doing everything right. She created a new Amazon account and provided the name of her landlord and her home address for shipping purposes. This way, her packages would arrive in the name of the property owner and she would stay invisible. She made sure that her name was not visible in any part of the order.

When prompted for payment, she used her real credit card in her name. She verified one last time that her name was not present anywhere within the actual order or shipping information. Her item, a pair of hiking shoes, arrived in the name of the landlord. Her real name was not referenced anywhere on the package. Within thirty days, she received a piece of mail that made her stomach drop. It was a catalog of hiking equipment addressed to her real name at her address. The company that accepted the order through Amazon was given her name as attached to the credit card. Therefore, the company added her to their catalog delivery list.

All of her hard work was ruined from this one mistake. Within another thirty days, she started receiving other junk mail in her name. Within ninety days, she found her name associated with her address online. This was her only slip. The lesson to learn here is that you can never tie your real name to your address if you do not want that association public.

I want to tackle Amazon purchases in three phases. First, we should discuss the anonymous Amazon account created in an alias name and funded with Amazon gift cards purchased with cash. This is your best option for private purchases. Next, we should acknowledge placing orders within your real name and delivered to addresses not associated with your home. This is the easiest way to avoid Amazon's strict fraud triggers. Finally, we should consider ways to sanitize our accounts, regardless of the names used, and understand how Amazon shares data with third parties. While this section is devoted to Amazon, I apply the same principles to other online retail businesses such as Apple, BestBuy, and others.

Anonymous Amazon Orders

The following steps will mask your real identity from your Amazon purchases. These have changed since drastically the previous edition. Amazon constantly receives fraud attempts with stolen credit cards used for purchases. Therefore, the scrutiny on every new account is high. We must convince Amazon that we are a good customer with legal money to spend. That should be easy, but we look suspicious as privacy seekers. Consider creating a new Amazon account with the following information.

- **Name:** Use the name of which you want your packages addressed. This could be the landlord at your address, or a completely new alias associated with your home. I prefer to keep this generic but not suspicious, such as Angel Martinez.
- **Email Address:** You must provide an email address for your new Amazon account. I recommend using an address attached to a custom domain as previously explained, which is forwarded to your ProtonMail account. I previously recommended a protonmail.com address, but this is no longer the case. Unfortunately, Amazon views these as suspicious and as an indicator of fraud. Custom domains previously unused on Amazon also receive scrutiny, but don't carry over bad history. Email addresses associated with forwarding or masking services will always be blocked. This is the first fraud flag analyzed by Amazon.
- **Payment:** My first preference is to purchase an Amazon gift card with cash from a local store. This is the least invasive option. I never recommend an initial amount higher than \$25. If you buy a \$500 Amazon gift card from a grocery store with cash, and apply it to a brand-new account, it is likely to be suspended as suspicious. A \$10 to \$25 card is less suspicious to Amazon, and less risk to both Amazon and you.
- **Address:** Provide your shipping address as desired. This may be your actual home if you do not have a better place for deliveries. If you are ordering large items, it can be convenient to have them delivered directly to your house. My preference is to have all packages delivered to an Amazon locker if you have one nearby. I have used my real home addresses in the past, but only for large deliveries. Because the name on the shipment is not my real name, I do not see this as a huge privacy concern. I believe it helps establish that someone else lives at your residence, and provides great disinformation. You should scrutinize any option you choose and make sure that it is appropriate for your scenario.
- **Telephone:** If forced to provide a telephone number, provide a VOIP option as previously explained. Make sure it is a number which is not publicly associated to your true name.

Be sure to document all provided details within your password manager. If there is an issue with your account, or it is flagged as suspicious, you may be asked to confirm any details provided at the time of account creation.

In a perfect world, you now possess a new Amazon account in an alias name with a small amount of funding. You should be able to spend your \$25 balance any way desired. Unfortunately, we do not live in this perfect world. In my experience, allowing the account to “mature” is your best option in order to avoid an account suspension. If you try to place an order right away for \$25 worth of SIM cards, expect failure. The following is my strategy.

- Create an Amazon account while connected to local public Wi-Fi, such as a library, Starbucks, or McDonalds. Do not use a VPN. We want Amazon to know the general location of your account creation.
- Apply a \$10 to \$25 Amazon gift card to the account.
- Browse through various products and add a small digital item to your cart. Do not complete the purchase. I recommend adding a digital download, such as a single song. At the time of this writing, I added the song “Willow” by Taylor Swift at a price of \$1.29. This further isolates my true music tastes from my new alias.
- In two days, visit Amazon again from the same public Wi-Fi without VPN and complete the purchase, deducting the amount from your gift card balance. This is typical behavior of a real customer, and not someone trying to steal from the company.

This purchase is very low risk to Amazon. If the funds were later deemed fraudulent, Amazon does not experience a loss of any physical product. After a week, your account should still be in good standing. Let’s move on to phase two.

- Attempt the purchase of a small physical product while connected to the same public Wi-Fi without use of a VPN. This item can be sent to your home or an Amazon locker, based on your own threat model and preference.
- If 30 days goes by without any issues, your account should now be ready for use.

This method should protect you from any association between your name, your purchases, and your home. You could likely use this new Amazon account for all of your purchases and have no problems. If you add Prime to the account, it usually further hardens the authenticity. My best advice is to always take it slow, keep the initial purchases low, and allow the account to mature as any other legitimate account would.

Once an account has aged a few weeks without issue, you could add a Privacy.com card as a payment source in order to avoid the need for future gift cards. That is what I do for clients. However, I always use a different billing address, such as a hotel. This is because I do not want the shipping address associated with the transaction. Providing a hotel billing address hides your shipping (home) address from any third parties who may have access to the billing data. This is always good practice any time you use a Privacy.com card since any provided billing

information is authorized anyway. **Never use your true home address within any billing details associated with an online purchase.**

After your account is established and “happy”, you should begin the process of connecting through a VPN. This action can trigger a fraud warning with Amazon, but this is rare if you followed the previous directions. I always connect my VPN through a server near the area where the account was established. If the account is locked, connecting through the original public Wi-Fi source should unlock the restriction. Once you can access the account from behind a VPN, you should never need to access the original Wi-Fi again. Be sure to always select the same general VPN location every time. If you typically connect to Amazon from a VPN server in Los Angeles, but log in one day from a New York server, except trouble.

If you have credit from gift cards on your account and it is suspended due to suspected fraud, your options are limited. Contacting customer support will usually not help. The only solution I have found is to contact “Corporation Service Company”, which is Amazon’s registered arbitration agent. To begin an arbitration proceeding, you must send a letter requesting arbitration and describing your claim to their registered agent at the following address.

Corporation Service Company
300 Deschutes Way SW
Suite 304
Tumwater, WA 98501

A polite, well-worded letter explaining your situation will usually unlock the account and funds within three weeks. More details can be found at the following website.

<https://www.amazon.com/gp/help/customer/display.html?nodeId=GNG9PXYZUMQT72QK>

I offer one final consideration before you proceed to the next page. Amazon facilitates most of their deliveries with freelance drivers in your area. Their drivers take a picture of each package using a personal mobile device connected to Amazon through their Flex application. The image is sent unencrypted through a public-facing URL and can be accessed without a password. This app requires Wi-Fi and Bluetooth scanning be enabled at all times, and it collects the details of any radio frequency transmissions, including your home SSIDs.

I refuse to allow strangers to take photos of my home, packages, and shipping labels from their phones. Because of this, I order all items to an alias name and have them shipped to a local Amazon locker. I respect that this is not always an option for everyone. The following pages tackle some privacy considerations for traditional Amazon purchases.

Traditional Amazon Orders

Another option is to have packages delivered in your real name to your UPS box. This way, you can use a traditional credit card without risk of exposing your home address. I have done this when I need to purchase expensive items which are monitored closely for fraud, such as a new cell phone or laptop. The more items which are delivered to your public box address, the more you establish history in your name at that address. Consumer reporting services may pick this up, which can be beneficial.

The only time I discourage this activity is when high-risk clients need to hide their general location. If a person is running from an abusive relationship, he or she may not want anything in their name within 100 miles of their true home. Consider your own needs. If you desire this level of extreme privacy, I believe you should avoid any deliveries made directly to your home in any name, including an alias. This prevents any spillage of real payment information in association with the home.

For an extra layer of privacy, I currently ship most important packages to an LLC name similar to a real LLC that I listed on my registration form with my local shipping provider. This prevents me from associating my real name with the purchases, and the LLC is not connected to me through the state. Let's run through an example.

- Assume I need to purchase a new laptop. Amazon would never send this out to a new account without much activity, especially if it is funded by gift cards or masked debit cards. Further, I want to place the purchase on my credit card in order to possess purchase protections.
- I have previously opened a mail receiving account with a local shipping provider under my true name. I advised that I own a business called Financial Ventures LLC, and I may occasionally receive a package addressed to the business.
- I have previously ordered a business credit card from American Express which displays both my true name and my LLC name.
- I create a new Amazon account under the LLC name and add my business credit card to the account. I provide true billing information, which happens to be my PMB address.
- I complete the purchase and instruct Amazon to ship the item to the independent shipping receiver or UPS box in the LLC name. Upon arrival of the product, I pick it up without incident.

In this scenario, Amazon never knows my real name, but only my LLC name. They see I am using a real business credit card which has a low risk of fraud. Third-party vendors never see my name, and only possess a CMRA shipping address. The billing is my PMB, which I have never physically visited.

Amazon Account Sanitization and Data Sharing

Regardless of the type of Amazon account you possess, you should consider minor modifications which can keep your data as private and secure as possible. After logging in to your account, consider the following.

- Click “Account and Lists” in the upper-right corner.
- Under “Ordering and shopping preferences”, click “Your Amazon profile”.
- Click the button titled “Edit your public profile”.
- Remove or modify any information desired.
- Click the “Edit privacy settings” tab.
- Uncheck everything in the section titled “What’s public on your public profile”.
- Enable “Hide all activity on your public profile”.
- Enable “Hide sensitive activity”.
- Uncheck “Allow customers to follow you”.
- Click “Account and Lists” in the upper-right corner.
- Under “Ordering and shopping preferences”, click “Manage your lists”.
- Hover over the three dots next to “Send list to others”, then select “Manage list”.
- Ensure list is “Private” and select “Don’t manage this list through Alexa”.
- Repeat for all lists on this page.
- In the Amazon search bar, click “Browsing History”.
- Click “Manage history”, “Remove all items from view”, then confirm.
- Change the toggle for “Turn browsing history on/off” to “Off”.
- Click “Account and Lists” in the upper-right corner.
- Under “Communication and content”, click “Advertising preferences”.
- Select “Do not show me interest-based ads provided by Amazon” and click “Submit”.
- Click “Account and Lists” in the upper-right corner.
- Under “Ordering and shopping preferences”, click “Your payments”.
- Expand any payment sources no longer used and select “Remove”.
- Click “Account and Lists” in the upper-right corner.
- Click “Login & security” and enable “Two-Step Verification”.
- Click “Account and Lists” in the upper-right corner.
- Under “Ordering and shopping preferences”, click “Your addresses”.
- Remove any sensitive content.

Identify your own Amazon-related requirements for convenience versus privacy and security. I confess I rely on Amazon heavily, but I am not proud of it. Spending cash at a local store removes the headaches associated with the previous five pages.

Does all of this really matter? I believe so. Consider one final anecdote. In 2021, I placed a purchase for a small home appliance on Amazon. I provided an alias name and had the item shipped to an Amazon locker. The billing address was a hotel and the form of payment was a Privacy.com masked debit card. The item arrived, but was non-functioning. I contacted the manufacturer, but they refused to honor the warranty. I provided a negative review under my alias announcing the issue. This allowed me to vent frustration and sprinkle some disinformation on the internet. I then moved on.

A week later, the manufacturer emailed me at the email address associated with my alias Amazon account (which was not the address used for my previous contact). They apologized for the problem and offered to send me a replacement in exchange for removing the negative post. They also offered to send the item to the original locker address or my provided hotel billing address. In other words, Amazon shared my alias name, billing address, physical address, and alias email account with the seller, even though the purchase was delivered through Amazon warehouses. I have since learned that this is common practice. Any Amazon seller can obtain user details with a simple request.

As an author, I noticed someone selling counterfeit copies of the second edition of this book. I complained to Amazon, and they removed the items. I then politely asked Amazon for the name, address, and email contact for the counterfeit seller, expecting refusal to disclose such personal details. Instead, they immediately wrote back providing the full account details. This led to some very interesting conversations with the counterfeit sellers.

As an attempt to push this further, I requested the name and email address of a person who posted a negative review of this book in order to compensate them for their troubles. Amazon happily forwarded me the personal Gmail account of the reader. This is completely unacceptable. When someone criticizes you for your usage of aliases with online orders, share these stories.

I realize this section offers many options without enforcement of a specific strategy. You should determine what is best for you. I will break down my preferred Amazon payment and shipping strategies in order from most private to least private.

- Order: Alias Name > Payment: Gift Card > Shipment: Amazon Locker
- Order: Alias Business Name > Payment: Gift Card > Shipment: UPS Store
- Order: Alias Name > Payment: Gift Card > Shipment: Home
- Order: Alias Name > Payment: Privacy.com > Shipment: Home
- Order: Real Name > Payment: Credit Card > Shipment: Amazon Locker
- Order: Real Name > Payment: Credit Card > Shipment: UPS Store

Moving Services

You will likely be asked to provide a credit card as a deposit when you reserve a company for any type of high value service. This may include home maintenance, satellite television, or movers. Many of these will not accept prepaid cards and will insist on a hold of funds within the credit card account. For these situations, I always recommend using your secondary credit card in an alias name. The following example illustrates the importance of not using a card in your true name with home services.

A client was relocating to another state to escape an abusive ex and to take on a new job. She was renting a small apartment near her new employer which included all utilities. She knew not to attach her name to anything regarding her new address. She contacted a popular home moving company and scheduled them to arrive at her current home, pack her belongings into a moving truck, and deliver them to her new address. As you can imagine, this presented a unique situation. They rightfully needed her current address and new address. They also insisted on obtaining her name, credit card number, and a telephone number to contact her during delivery. She panicked and hung up without giving them any details. Then she called me.

If she had completed the order, there would be a very strong trail from her previous address to her new address. I suspect that within weeks, she would receive targeted advertising in her name at her new address offering typical services to a new resident. Many moving companies supplement their revenue by sharing customer databases with non-competing services which cater to new residents. This data could easily leak to online people search websites. I decided to help her by facilitating the entire moving process on her behalf.

I chose U-Haul as the most appropriate mover for her situation. Her relocation was substantial, and the mileage fees alone for a moving truck were outrageous. When adding the fee for two movers to facilitate the transfer, the quote was several thousands of dollars. I completed the order for the move in three isolated phases. For the sake of this scenario, assume that she was moving from Miami to St. Louis.

I scheduled U-Haul to deliver two moving U-box containers to her current home. These are large wooden crates which allow you to store belongings before being shipped by a semi-truck and trailer. U-Haul required a valid credit card so I provided my client's secondary credit card in an alias name. This order also included pickup of the full containers and storage at the Miami U-Haul headquarters. The boxes were delivered by the local Miami U-Haul provider closest to her home.

She had friends help her fill the containers and I called U-Haul to come and pick them up. They were transferred and stored at the Miami headquarters awaiting further instruction.

Customers are allotted 30 days of included storage before additional fees are introduced. I called the Miami U-Haul and provided the order number and alias name. I requested that U-Haul deliver these containers to the St. Louis storage facility. I was given the rate for this service and a deposit was charged to the card on file.

A week later, the email address on file received a confirmation that the containers had arrived in St. Louis. They were stored there awaiting further orders. The storage fees were covered as part of the original contract. Through the U-Haul website, I identified a reputable moving company. I added their services to the current open contract and provided a destination address of a post office within the city near where she was moving. This was the last piece of information that was given to U-Haul. I authorized U-Haul to release the containers to the moving company.

I called the independent moving service that would be picking up her containers and delivering them to her new apartment. I provided the order number and her alias name. I stated that the original order had a placeholder address because I did not know the new address to where I was moving. I then gave this company her actual address over the phone and she met the movers there to direct them with the move. She possessed the release code that allowed the moving company to close the contract and be paid by U-Haul.

Out of curiosity, I input similar beginning and ending addresses within the U-Haul website moving calculator. My method was the exact same price as if I would have given U-Haul everything they needed in one step. In my method, U-Haul does not know her real name or her current address. For full disclosure, they know that she likely lives near St. Louis. There is very little value in this information to U-Haul. The independent moving company knows her new address, but they do not know her name or from where she moved. If her U-Haul account were to be breached, her address would appear to be a local post office.

I trained her to have small talk answers ready for the movers. She was to say that she is staying in St. Louis with her husband while he was assigned there by his employer and then returning to California soon. I later asked her how that went. She stated that she simply did not answer any of their questions and they stopped talking to her altogether. I liked working with her.

As you can see, every step of any relocation is full of potential vulnerabilities. One mistake can unravel all of your effort. Plan everything to the point of exhaustion. Attempt to find areas which may present hurdles. Run through every possible scenario and consider any ways in which your privacy may be in jeopardy. Again, this is a lot of work. However, the payoff at the end is worth all of the hassle.

Appliance Purchases

During a move, it is likely that you will need some major purchases delivered to your home. There is no room for error here, as most big-box stores collect and share data about all of their customers. When you purchase a refrigerator, washer, dryer, or other large item, free local shipping is often included. In order to complete the delivery, the store will require your home address, telephone number, and a name. The address must be accurate, but you could provide a burner phone number and an alias name. However, the name provided must match the source of payment. If you use a real name or accurate credit card, you have just connected your true identity to your home address.

In previous books, I have mentioned the ability to make the purchase under an alias name with a secondary credit card, but I no longer have faith in the protection this provides. In 2017, I needed to purchase a replacement oven for a non-functioning unit. I had agreed to complete this task for my landlord as part of his willingness to allow me to stay there anonymously. I walked into a national chain appliance store and identified the model I desired. I had no way to transport it to my current rental unit. During checkout, I provided my alias name, which also appears on my secondary credit card. When the sales person swiped the card, he asked if any of the names on the screen were me. The first option was Michael Bazzell. Since I am always concerned about protecting my home address, I awkwardly canceled the order and left without completing the purchase. Fortunately, I had not yet provided the delivery address. This was a close call.

What happened was a careless mistake. On a previous visit to this chain at another location, I used my real credit card under my real name to make a small purchase. This entered me into the nationwide system. Since my alias secondary credit card possessed the same account number and expiration as my primary card in my name, the store knew both purchases were connected to the same card. The system queried the card number and prompted the sales associate to choose any applicable names of previous customers. Some stores do this with telephone numbers. While this may seem minor to your threat model, it was a serious violation to me. Today, I conduct these purchases quite differently.

I first visit the store to identify the exact appliances I desire. I make sure that my choices are in stock and ready for delivery. I choose businesses with powerful online stores such as Lowe's and Home Depot. I then leave and decide which level of privacy I desire for me or my client. I present two options here, displayed in order of most private to least.

If possible, I make the payment in store with cash. I then provide the real address for delivery and any name I choose. Some stores will not accept cash over a specific limit and will decline a large purchase. While the money displays "legal tender", private businesses have a right to refuse cash. My next option is prepaid credit cards. I purchase enough gift cards to cover the

entire amount, and again provide the real address with an alias name. This has worked throughout most of 2017 and 2018. Lately, I encounter stores that require government identification in order to schedule a delivery. This is a deal-breaker for me. When I receive this level of verification, I move to the second option.

I make the purchase through the store's website using a Privacy.com debit card number. We lose a small amount of privacy here because there is a digital trail back to my bank. This is acceptable for most clients. After the online purchase is approved, I telephone the local store and schedule the delivery. Since I am not there in person, there is no way to enforce a check of identification. The delivery people could ask for it, but this has never happened. If it did, I would simply claim that I didn't have one with me, as I was not told this would be a requirement.

Using Privacy.com debit cards online is not always possible. Beginning in late 2018, I noticed more online stores were declining debit card numbers generated by Privacy.com. This is because these numbers are clearly tagged as an anonymous payment type, similar to a prepaid card. When a merchant processes a payment with one of these cards, it may have rules that decline the purchase completely or if above a specific amount threshold. This has happened to me, but there is always a workaround.

I attempted to purchase a refrigerator from Home Depot through their online website. I knew it was in stock locally and I planned to have it delivered at no cost. I provided my real address, the name of John Wilson, and a VOIP telephone number assigned to my home. The purchase was immediately declined. I knew that the Privacy.com card I was using was valid and had not been used with any other merchants. The Privacy.com app did not display any declined charges. A call to Home Depot customer support only revealed that the purchase was declined, with no further explanation.

I called the local store, and asked to speak to someone in the home appliance division. I explained that I tried to make a purchase online, but that it was declined. I told the employee that I contacted the bank that issued the debit card and was told there was no attempt to process the charge from Home Depot. I then asked if they could do this manually. The employee agreed and processed my order over the telephone. I provided the same Privacy.com card number, alias name, and actual home address. The charge was processed with no issues, and I could see the transaction within the application. The refrigerator was delivered two days later without incident, and I was never asked to display identification. The receipt was scanned into a PDF at the store and sent to my ProtonMail email address assigned to my home.

I should note here that a Privacy.com account has an initial purchase limit of \$300 per week. This will not suffice for large purchases. Once you routinely make small successful purchases using this service, your limit will slowly rise. I have found that a call to their support can lift

that limit higher. I have clients who are allowed to spend up to \$2,500 weekly with a monthly limit of \$10,000. It takes time to build to this level, so I suggest using the service long before it is needed for expensive purchases.

Overall, I never associate my true name with any delivery to my home address. This includes products paid for using a secondary credit card which could easily be tied back to me. In the first scenario (cash or prepaid cards), my weakest link is the surveillance footage of me in the store. If they demand government identification, this option cannot be made private and should be avoided. In the second scenario, the Privacy.com card is my threat. Privacy.com knows my name and that I purchased an item at a specific store, but does not know my address. The store knows I purchased with a Privacy.com card and my address, but does not know my name. The bank knows I spent money through Privacy.com. A court order to all three would reveal the connections. For most clients, that is not a violation of their threat model. For a rare handful, it is. Consider the following situation I had with a client.

In 2018, I helped a client who was an ex-wife of an FBI agent who had begun harassing her online and in real life. She worried that his access to premium data mining tools and government databases placed her at an increased risk. When she purchased her appliances with delivery to her new anonymous home, she ordered one item at a time, always paid cash, and politely declined to display any identification during each purchase. She is a focused, strong woman who can tolerate awkward moments and silence. Her cold stare magically bypassed the ID requirement each time. She is a ninja, so your mileage may vary.

Some clients express concern over the warranties which come with appliances. Large items often include a warranty card which must be mailed to the manufacturer. It asks for your name, address, and telephone number, along with a serial number of the appliance. My clients ask if they should use their real names since a warranty in an alias may create a situation where payment cannot be processed. My firm stance is that these cards should be avoided. They are not required for the warranty to be active, and seldom change any of the coverage. Your receipt from the purchase will satisfy any requirements, and the date on the delivery receipt defines when the warranty begins.

When I had a clothes dryer stop working within the warranty period, I simply called the local store where it was purchased and requested a warranty repair or return. The store was able to view my purchase history under the alias name and accurate address. The store created a service ticket, and a third-party repair company contacted me. They responded to my home the next day and repaired the machine. They already possessed my alias information because Home Depot shared it with them. This did not surprise or concern me, as it was an alias name. This is another example of how any details provided at the time of purchase can be shared without your knowledge. Your diligence with anonymous purchases will protect your home address from being publicly exposed.

Medical Services

This section presents quite a quandary. Until this point, I have encouraged you to hide your true identity during purchases in order to protect your personal information from being released publicly. Medical services can complicate this rather quickly. Your doctors need to know your true identity in order to update health records which could be vital to your life. Health insurance requires confirmation of your identity including photo identification and an SSN. We are often told by medical staff that HIPAA laws protect our information, but the countless healthcare breaches prove this line of thinking as incorrect. We know that any information provided during receipt of medical services is likely to be stored insecurely, shared intentionally, or leaked accidentally. Therefore, let's clean it up.

If you need emergency services, surgery, or typical care from a physician, I believe you should absolutely provide your true name and DOB. This will be used to modify patient records, and during any follow-up care. For me, the personal details stop there. I never provide my SSN, home address, personal email address, or telephone number in any circumstance. The following actual events should summarize my reasons.

In 2017, I visited a local optometrist for an eye checkup. I provided my real name and a slightly altered DOB. I refused all other details and paid with cash. The office insisted I provide a cell number as it was the system identifier. I supplied an old Google Voice number which was no longer used. Within 90 days, I began receiving marketing text messages related to eye care. Today, my true name is associated with that phone number within a marketing database titled "U.S. Consumers" provided by infousa.com. I can do nothing to remove it. Fortunately, the DOB and contact information does not jeopardize my privacy.

In 2018, I responded to a local urgent care facility due to suspected pneumonia after extensive international travel. I provided my true name and DOB on the patient paperwork. I supplied a VOIP telephone number, a CMRA mailing address, and a burner email address. I left the SSN line blank. When pushed for my SSN, I explained that I was paying cash and that I had not met my (high) deductible on my health insurance. I was treated, medicated, and released. In less than 90 days, I received an email to my burner account from "DrChrono" urging me to get a flu shot at the same urgent care facility where I was previously treated. It referenced a high number of flu-related cases which can lead to pneumonia. DrChrono is the software solution used by many urgent care facilities to collect and update patient information. I never agreed to provide my name, email, or location to this third party, yet it was shared. I still receive targeted advertising from that visit. Should I really care about this company knowing my medical history? I believe so. If you disagree, consider the following verbatim wording from their privacy policy.

“We use information, including Personal Information, for internal and service-related purposes and may provide it to third parties ... We may use and retain any data we collect to provide and improve our services ... We may share any information we receive with vendors and service providers ... If we are involved in a merger, acquisition, ... your information may be sold or transferred.”

In other words, they can do anything they like with your medical data. Worse, the collection of data is more likely to be breached or leaked publicly. The next week, I responded to a local pulmonologist for follow-up to my issue. As expected, they demanded many personal details. I provided a unique email address and VOIP number as well as the same CMRA mailing address. I attempted to leave the SSN line blank, but I was challenged. I was informed that this was mandated by federal law (which is not accurate) and required from insurance providers (which is also not true). My line about my deductible was not getting me anywhere. The compromise I made was to supply my health insurance account number, which could be verified on my member card. The office staff hesitantly accepted this.

In 2019, I was sent a notice from this office notifying me that the physician I had seen was retiring. I didn't think much of this as he was not someone I planned to visit again. Three weeks later, I received promotional emails and text messages from other area doctors who could take over for any related medical needs I had. I assume that the original office sold their patient contact data to similar offices before shutting the doors permanently. This was likely a HIPAA violation.

If you are often forced to provide an SSN for medical treatment while paying with cash, you have an alternative option, which enters some grey area. You could apply for an EIN from the IRS. I have a client who has done this. He grew tired of the battle to exclude his SSN from new paperwork with every visit. He applied for a Sole Proprietor EIN from the IRS (explained later), which was approved instantly and included a confirmation letter from the IRS displaying this number. He now provides this EIN, which is the same number of digits as an SSN, on all of his forms. He also provides his insurance card which displays the unique number assigned to him for any claims. The medical offices have no idea that the number he provides on the SSN line is actually an EIN. Both pass validation. Since he owns that number, he is not committing fraud. However, there could be some issues with this.

If his insurance provider receives notification that treatment was conducted for a person with the EIN he supplied, the claims could be denied. Some medical services only include the insurance ID number within claims while other place priority on the SSN. If he were challenged by his insurance provider, he could provide proof of the ownership of the supplied EIN, and could say that he accidentally gave that instead of the SSN. I only tolerate this strategy for those with minor medical needs. Do not risk continuous treatment over SSN formalities such as this. Tread carefully, your health is more important than privacy measures.

HIPAA Disclosure Considerations

When we visit a doctor, we are bombarded with forms and releases. These offices know that most patients do not read or understand the documents. We simply sign the final page and hope for the best. Under HIPAA laws, your health care provider may share your information to the extent which you authorize the sharing. A health care provider may share relevant information if you give permission; you are present and do not object to sharing the information; or you are not present, and the provider determines based on professional judgment that it is in your best interest. This is a lot of power over the sharing of your medical data. Each office will present documents which request your approval to share your medical information when the office deems justified.

There are many legitimate reasons why a medical office would need to share your details. If you are sick and your family wants to discuss your care, you would need to allow sharing of your diagnosis. Doctors often communicate with pharmacies about your medication. However, this information can also be abused, especially when considering relationships to third parties. I encourage you to take a closer look into these forms and consider the following.

- You have a legal right to receive a paper copy of any HIPAA form. I always demand my own copy of anything I sign.
- Documents such as the “Disclosure of Personal Health Information (PHI)”, “National Health Information Network (NHIN)” and “Health Information Exchange (HIE)” forms are optional. These acknowledge your informed consent to share your information. Per HIPAA law, you can decline signing these forms and medical treatment cannot be withheld.
- If you have already signed a form, you are permitted to revoke your signature.
- If an office has combined all documents into one long form, you can cross through any provisions for the HIPAA notice which you do not authorize. If desired, you can include wording similar to “I do not agree to HIPAA notices due to disclosure language”.
- Each U.S. state is a member of the Nationwide Health Information Network (NHIN). Your data is likely included within this program unless you choose to opt-out. You can request a “State HIE opt-out form” from your doctor. If you complete this form, your information can no longer be shared through this database.

There is a delicate balance here. Every time I have challenged the requirement to authorize release of my data, I see the eye-rolls. I can hear the annoyance within their voice. I get it. I am the difficult patient for the day. I believe this effort is justified, but you may disagree. Never avoid necessary medical treatment because an office does not understand HIPAA laws and is requiring you to sign away your rights. Choose wisely.

Store Memberships

I meet many clients who rely on store memberships for much of their shopping. These include places such as Costco and Sam's Club, both of which usually require a paid membership in order to buy items. The membership process is quite invasive. These businesses typically require your name, home address, cellular telephone number, personal email address, payment details, and a stored copy of a government issued ID. Even if you pay with cash, they demand a valid credit card number within their files. Some stores demand a new photo of you, which is kept forever.

My easy solution is to simply avoid these traps. I have not entered a store which required a membership in over twenty years. However, that may not work well for you. If you insist on shopping within these businesses, please consider the following.

- Most stores allow entry if you possess a gift card from the business. If you know someone with a membership to Costco, they can purchase gift cards within the store. You can enter and spend the balance of this card without an active membership. If purchasing with cash, there should be no trail.
- Most stores require automatic renewal of the membership. You can usually opt-out of this by contacting customer support. Otherwise, renewals keep your membership active, even if under a different credit card number. If you are issued a new card under the same account, most businesses are allowed to retrieve the new billing details. Switching the payment source to a masked debit can prevent this. Disable any cards which should no longer be charged.
- If you have an active account, you can contact customer service and demand that your government issued ID number, such as a driver's license number, be removed from your profile. Any digital scans remain, but this may remove a unique identifier which will be shared with numerous third parties.
- You have the right to opt-out of marketing mailings, calls, texts and emails. A call to customer service should offer this option. Call each time you continue to get bombarded with unsolicited communications.
- These businesses will not delete any stored information within your profile, but you can modify the details. Updating your contact information to a "burner" address, phone, and email may prevent abuse of your real information. A call to customer service should offer this option. Never ask to "remove" any details, as the customer support representative likely does not have that authority. Always refer to "updating" your record in order to continue to be a valued customer.

Anonymous Purchase Complications

I have experienced many failures while attempting anonymous purchases. Beginning in 2018, I started seeing a huge increase in blocked payments, especially if ordering physical products via the internet. When using a VPN connection, burner email address, alias name, and VOIP telephone number during an online order, I found many purchase attempts blocked by various fraud prevention strategies from the merchant. My orders were canceled without explanation. This happened even when using a legitimate payment source. Since then, I have documented the following most common traits of anonymous payments which seem to trigger fraud prevention systems.

- **VPN:** A VPN alone will usually not flag a payment as fraudulent. In my experience, there must be additional factors before this makes an order seem suspicious.
- **Name:** If using a legitimate credit card, the name must match perfectly. If using a secondary credit card, the alias name must also be exact. Your credit card company discloses to the merchant if the name is different than on the account.
- **Email:** If using a known temporary email provider (such as Mailinator) or masked service (such as 33Mail), this will cause scrutiny. In my experience, legitimate alias email options from ProtonMail and Fastmail will be accepted. Credit card providers do not always confirm registered email accounts with the merchant.
- **Address:** Providing a shipping address different than the billing address causes scrutiny. If the shipping address is a CMRA or PO Box, expect even more hesitation. Combine a UPS box with a billing address in another state, and you should expect a blocked payment and canceled order.
- **Telephone:** When you make a purchase with your credit card, you are asked for a telephone number. The merchant will be notified if that number does not match the number associated with the credit card account. Therefore, I attach secure Google Voice numbers to my credit cards associated with my real name and secondary alias names. I then provide the appropriate number on all orders.
- **Prepaid Cards:** I only use these for purchases inside physical stores. Online use requires registration and often an SSN. Online orders with a prepaid card will be blocked without proper registration.
- **Masked Cards:** Companies know when you pay with a masked card such as Privacy.com. Many online merchants will block purchases unless the billing name matches the shipping name, and the shipping address matches public people search records.

The following examples summarize actual successes and failures when ordering products through online merchants.

- I attempted to purchase several refurbished iPhones directly from Apple. I provided a legitimate Privacy.com card number, alias name, and UPS store address. The order was canceled due to “high risk”. Talking with the Apple security team revealed that the suspicion was because the name provided did not specifically match the payment source or address. While Privacy.com allows you to use any name for purchases, merchants can block these payments due to lack of a confirmed name through public records and online databases.
- I attempted the same type of purchase through Gazelle. The order was canceled immediately. Fraud prevention personnel confirmed that the cancellation trigger was because the payment source was a masked debit card. They confirmed they would not accept any prepaid or masked card which were not registered to a real name, address, and SSN.
- I attempted to order several discounted new iPhones through BestBuy. I provided my secondary credit card in an alias name, a shipping address of a UPS store, a VOIP number, and an alias ProtonMail email address. The order was canceled because the telephone number did not match the number associated with the secondary credit card, and the delivery address was in a state different than the billing address.
- I attempted another purchase directly through Apple. I used my secondary credit card, exact alias name displayed on the card, exact billing address (PMB), a UPS store shipping address, and the VOIP number on file with the alias credit card. The order was accepted, but held for review due to the shipping location being a UPS store in a different state than the billing address (PMB). Apple demanded a call to me at the number on file with the credit card. I answered the call (forwarded to MySudo) and confirmed all aspects of the order. The phones shipped the next day.

The lessons learned are as follows:

- Many online merchants will not ship products when using masked or prepaid payment options. Calling a local store will usually bypass this restriction.
- Merchants will accept traditional secondary (alias) credit cards if all provided information matches records provided by your credit card company.
- Be prepared to accept a call at the number provided during purchase, and make sure that number is on file with your credit card provider.
- When an order is canceled, call support and challenge this annoyance. Often, orders are canceled due to suspicion of fraud, and the merchant assumes that a criminal will not challenge the decision. Contacting a human over the telephone often eases the level of concern for fraud. You can request that the card used be “whitelisted” for another order attempt. If approved, you can then repeat the purchase and hope for a better result.

Device-Specific Complications

When you connect to an online merchant, details about your connection are shared with the website provider. This can include information about your device such as the operating system, installed fonts, and browser configuration. Many fraud prevention systems analyze this data during the purchase in order to identify fraudulent orders. Unfortunately, it is easy for us to get caught-up in this dragnet. My research identifies the following complications.

- Placing an order from any Linux operating system with a hardened Firefox browser triggers fraud detection with numerous online retailers.
- Mobile operating systems such as iOS and Android appear less suspicious than typical operating systems such as Windows, Mac, and Linux.
- Purchases submitted through Android virtual machines almost always trigger order suspensions.
- Purchases submitted through Windows and Linux virtual machines often trigger order suspensions.
- Purchases submitted from browsers with a large amount of internet activity have a higher success rate than those placed from browsers with no personal usage.
- The stock Chrome browser is trusted more than any other options, including Firefox.
- Purchases submitted from Google Chromebooks or iPads appear less suspicious than all other options presented here.

Post-Purchase Considerations

Over the past few years, I have witnessed a concerning interaction between the merchant and customer after a purchase has been made. This is usually in the form of an unsolicited text message or email from the merchant asking for feedback about the purchase. These are extremely common in the service industry, including everything from home repairs to medical appointments. Consider the following two scenarios which jeopardized the privacy of my clients in 2019.

“Joan” purchased a WordPress plugin for her online business. This premium option allowed her online blog to easily accept credit card payment for a niche product she provided for sale. During checkout, she supplied her real name, credit card details, burner email account, and the PO Box address near her private home. Joan was not under any threat of physical violence, but desired a basic level of privacy. There was no public online documentation of the city and state where she resides (yet). Within minutes after the order, email messages began arriving about her purchase.

The first was a welcome message explaining use of the product and the required license key. Immediately following, she received an automated email from a sales representative requesting feedback about the purchase. She ignored this message. The next day, she received an email message asking if there was something wrong with the purchase. The wording insinuated that a confirmation was required in order to use this product, and specified that they had not heard from her since the purchase. She responded “Everything is working fine for me, No issues”.

She immediately visited the website to make sure she could still log in to the portal, and noticed something inappropriate. On the home page of the site, a section titled “Happy Customers” displayed a scrolling list of people who had recently purchased this plugin along with a brief snippet of feedback. For Joan, it displayed her first and last name, city and state, along with “Everything is working fine for me, No issues”. She was appalled and immediately contacted the company demanding removal of the content.

The response from the company was that this was standard marketing, and that she agreed to the use of her information. The employee provided a link to their privacy policy page, which indeed included wording about use of customer feedback on the site. Joan’s approximate location was now publicly visible to the world. It was eventually overridden with more recent feedback.

“Mark” visited a new dentist for a routine exam. He was new to the area after he relocated to an anonymous home upon receiving numerous death threats and a violent physical attack. He chose a dentist in the town adjacent to his home, and used his real name to make the appointment. He provided a PO Box as an address, VOIP number for his cell, unique ProtonMail account for his email, and paid with cash. It is important to note that Mark’s real first name is very unique, and there are only a handful of people in the country with that first name. This will work against him in a moment.

Days after the exam, Mark began receiving text messages from the dentist’s office in reference to his visit. They were requesting feedback from him in an effort to provide the best experience possible for all patients. He ignored these, but they kept coming. They started with, “We would like your feedback”, became more aggressive with, “We still need you to respond”, and finally became invasive with, “Your input is required”. Mark finally responded to the messages in order to make them stop. He submitted something very generic such as “Great visit”. The messages finally stopped.

Several days later, Mark conducted his weekly search of his name on Google. He does this to identify any new threats toward his privacy. He used the “Past Week” option in the “Tools” section of Google in order to filter results to only those posted in the past week. The first result made his stomach drop. It was a review site for the dentist Mark had visited. One of the recent reviews was, “Great visit”, and it was attributed to Mark’s real first name and last initial.

The page clearly identified the city and state where the office was located, and Mark was now publicly exposed online.

Some may think this is no big deal, but I feel different. The service requesting feedback from Mark never asked for consent to publish the information. This may have been included in the paperwork signed at the office, but Mark could not recall any wording associated with this action. Publishing the first name and last initial would be less invasive to a person like me (Michael B.), but Mark's real name is immediately distinguishable at over 15 characters. Anyone searching his name now has a great starting point to find his home, as very few people visit a dentist while on vacation.

Fortunately for Mark, I was able to have the feedback removed. I first contacted the dentist's office and made a polite request on his behalf. The office staff informed me that they do not have control over that data, and that they hire a third-party company to send those messages, collect the content, and publish to a dental review site. I contacted the business providing this service and repeated my request. I heard nothing back from them, and had my attorney draft a cease and desist letter to them demanding removal of the information or accept the risk of civil litigation. The content was removed the next day, but I never received an official response from the company. A letter from an attorney is most often a bluff, but usually not worth fighting. Paying an attorney \$100 to send an empty threat is often the most successful strategy we can apply.

You have probably received similar messages from a merchant after a payment. With the popularity of review websites such as Yelp, TripAdvisor, and many others, businesses want to stay ahead of any negative reviews. By convincing happy customers to submit positive feedback, they often have a legal right to publish the content you provide. These positive reviews help drown out the negative feedback initiated by unhappy customers.

I believe there is never a reason for a privacy-conscious person to provide any type of review or feedback in any form. Whether directly to the merchant or on a third-party website, you are exposing potentially sensitive information when you volunteer any details about your purchase or experience. Furthermore, you have nothing to gain. The only party which benefits from your feedback is the merchant.

In most scenarios, merchants are hiring third-party companies to send these messages and collect the data. You have no control over the ways this data is abused. A breach, leak, or intentional sale of the data could expose you to numerous online people search websites. The simple solution is to never participate in this activity.

Customer Support Considerations

I am of an age which I recall contacting a company's customer support by picking up my landline phone and calling a toll-free 800 number which was immediately answered by a human. Those days are over. Many online companies no longer offer any type of telephone support, and a few have eliminated email contact options. The latest customer support protocol forces many customers to use a chat application embedded into the company's website. You must participate in this text-only support option if you want any chance at a remedy to your issue. There are many privacy and security concerns with this activity. Consider the following personal experiences.

- While chatting with a representative from Amazon, I could load all of my previous conversations with other customer support individuals. I also confirmed with the current representative that she could see every support conversation ever associated with the account. I was told this data cannot be deleted and will permanently be present within my profile. She also confirmed that future chat sessions will present all previous content to the next employee. I suspect they use this history to make decisions about refunds and exchanges, so be polite.
- While chatting with support from a financial software company called Banktivity, I was asked to send a screenshot of sensitive bank details through their "secure" portal. This data was stored within a publicly-available third-party file storage host which was immediately visible to anyone with the public URL. After I filed a complaint, customer service told me this was very secure and I should not be worried about the exposure. After seven demands over a 10-day period, I finally was able to force the company to remove the data from public view. Anything you upload through these chat portals is very likely exposed publicly if someone is able to identify the direct link. In this scenario, Google was indexing the domain used to store the sensitive data, so retrieval was simple. I encourage people to avoid any financial-aggregating services such as Banktivity, Mint, QuickBooks, etc. and never upload any sensitive files through these customer support options.
- Your comments within a customer chat service may be used against you. I have witnessed compliments from a customer be repeated on website landing pages attributed to the full name of the person. On the other end of the spectrum, I have witnessed clients' comments within chat windows be used against them. One client engaged in a text argument about an order which became very heated. The company sent out a Tweet with a screenshot of the communication in effort to shame my client. Overall, assume everything typed or spoken to any customer service representative will become public information. While this is unlikely with reputable companies, it helps us ensure that we are never caught off guard after a dispute.
- I simply never engage in any customer service from my true name. I always use an alias for the order and any follow-up communication.

Virtual Currencies

You may question my reasons for excluding virtual currencies, also known as cryptocurrencies, such as Bitcoin, from the beginning of this chapter as a private payment option. First, I have found many services to be too complicated for most of my clients. Second, possessing truly anonymous digital currency can be quite complicated. Let's begin by defining virtual currency. It is a type of unregulated digital currency which is issued and usually controlled by its developers. It is used and accepted among members of specific virtual communities. The most popular, and most widely accepted, is Bitcoin. Next, we should acknowledge the typical route most people take to purchase this digital money.

Most people who own any type of virtual currency purchased it through an exchange. You might create a profile, provide a credit card number, and purchase a specific amount of Bitcoin. The currency is placed into your "wallet" which is maintained at the exchange. You can now spend this money anywhere which accepts Bitcoin. The merchant does not know your identity, and the Bitcoin is "anonymous". However, there are many concerns with this strategy.

First, the exchange will demand to know your true identity. You will be forced to upload government ID and third-party verification systems will confirm any inaccuracies. Next, the exchange will maintain a record of all purchases. A subpoena to them would disclose all of the activity associated with your name. After that, the publicly visible wallet identifiers disclose the exchange service you use. Finally, you are at the mercy of the security practices of the exchange. Numerous companies have suffered data breaches which lost all of their customer's money. All of this takes away any privacy benefits of virtual currency. I believe all exchanges should be avoided if you want true anonymity.

I prefer to control my own locally-stored Bitcoin wallet. This can be done with **Electrum** (electrum.org), an open-source software application which stores, accepts, and transmits virtual currencies directly from your computer. Let's walk through installation and transmission of Bitcoin through Electrum. You can download the software from their official website. It natively supports Windows, Mac, Linux, and Android, and the installation is straightforward. Next, we need to create a wallet.

- In the Install Wizard, click the "Choose" button to identify the default directory.
- Click "Cancel" and enter the desired name of your wallet and click "Next".
- Choose a "Standard Wallet" and click "Next".
- Select "Create a new seed" and click "Next".
- Accept the default seed type and click "Next".
- Copy the words presented into a password manager for safe keeping and click "Next".

- Paste the words into the next screen to confirm receipt and click “Next”.
- Choose a secure password, enter it, and store it in your password manager.
- Click “Next” and close the application window.
- If desired, move your wallet file to a more secure location.
- Open the application and ensure you can access your new wallet.

Congratulations, you now have a Bitcoin wallet. However, you have no Bitcoin. This is the hardest part. If you cannot buy virtual currencies from an exchange, how do you get any? Some people use Bitcoin ATM machines. You can insert cash and provide a Bitcoin address for deposit into your account. The disadvantages are a 5% to 10% fee for this service and the potential of making a mistake and losing any money. Furthermore, many people report machines requiring you to take a “selfie” while holding your ID, which I would never recommend. However, if you have a local ATM and want to experiment, here are the instructions.

- In the Electrum application, click the “Receive” button at the top of your wallet.
- Copy the receiving address, similar to “1IKIV7Anhsv15RXYS7X2HR2ijjMV7BzIsI”.
- Enter a description of the transaction, such as “ATM” and click “Save”.
- Click the barcode to enlarge and print the visible barcode.
- At a Bitcoin ATM, follow the prompts to scan your barcode or enter your Bitcoin address, enter the amount of purchase, insert your cash, and confirm your deposit.
- In a few moments, you should see a pending deposit within the Electrum app.

There are a couple of things to explain further. Electrum needs internet connectivity to connect to the Blockchain in order to update any transaction records. Many ATM machines demand a cellular telephone number in order to send a text message containing a code which needs to be entered into the ATM. You could use a VOIP number as explained earlier, but this now associates the transaction with that number. For this reason, I try to avoid ATM machines unless I need the funds available right away. The confirmed Bitcoin deposit can take hours to become available within your wallet.

My preferred way to acquire Bitcoin is from another individual. This can be accomplished in a couple of different ways. The best option is to provide a service which can be paid via Bitcoin. For several years, I provided an online training program which accepted Bitcoin. This helped generate my first few Bitcoin transactions and allowed me to build up my wallet of funds. If you have an online service that caters to privacy enthusiasts, accepting Bitcoin can benefit both you and the consumer.

Technology, hacker, and even Bitcoin-themed conferences are common in urban areas. These events usually include a Bitcoin party where virtual currency enthusiasts gather. One purpose of this interaction is to buy and sell Bitcoin. Many people will happily sell their Bitcoin for cash while buyers see this as a great opportunity to obtain fairly anonymous money. Be careful. Make sure there is a trusted mediator present to ensure the transaction goes through. It is important to have access to your wallet in order to verify the transaction. Ask other attendees about trusted sources and identify someone with whom you feel safe making an exchange. After attending a few events, you will get a feel for the reputable providers. The process within Electrum is identical, and you would give the seller the address or barcode.

Let's assume you now possess some Bitcoin. What should you do with it? For most of my clients, not much. Less than 5% of my clients possess any virtual currency. Of those, very few ever spend it. The most common uses for cryptocurrency are online services and exchanges. You can buy a VPN service, ProtonMail account, or online storage solution with Bitcoin without disclosing a true name or credit card. However, very few physical retail locations accept it. I keep Bitcoin available at all times in order to anonymously purchase these types of online services for clients. Paying via Bitcoin removes most identity verification demands. In order to spend Bitcoin stored in Electrum, the following should assist.

- Click the “Send” option at the top.
- Enter the Bitcoin address provided by the service you are purchasing.
- Provide a description and amount.
- Click the “Send” button.

Be careful with the amount. You can use various online conversion utilities to display the amount of Bitcoin in USD, or you can add USD as an option directly within Electrum. The following modification in the software adds USD in the send, receive, and balance menus.

Tools > Electrum Preferences > Fiat > Fiat Currency > USD

Any virtual currency you possess in this wallet is your responsibility. If you delete the file or lose access, you have lost any money inside it. It is estimated that 23% of all Bitcoin has been lost due to inaccessible wallets. Please do not become part of this statistic. Overall, most of my clients have no use for Bitcoin. I only recommend these actions if you truly NEED it. This is especially true if the volatility of Bitcoin is concerning to you. My first Bitcoin transaction was in 2013 at a rate of approximately \$30 per Bitcoin. While writing the previous edition of this book, that same Bitcoin was valued at over \$5,000. Today, it is over \$50,000. Next year, it could be worthless. To be fair, values of the U.S. dollar and gold could also plummet. Personally, I view Bitcoin as a tool and never an investment.

Two Gold Coins

While traveling internationally, I always keep two one-ounce gold coins in my possession. Cash may be king, but foreign currency during international travel may not carry much weight. However, gold is typically respected with global rates of value. I have found that two ounces of gold can get me out of any uncomfortable situation I may experience. At the time of this writing, two ounces of gold has an approximate value of \$3,500 USD. When including various fees associated with sales, I would expect to be able to convert these coins into \$3,000 worth of local currency at practically any destination. This would easily allow me to purchase airfare with cash in order to return home or wire money to a credit card in order to extend spending power. If I find myself in a corrupt part of the world, a gold coin can ensure me safe passage through an international checkpoint. That story is probably better suited for another book.

Prior to 2019, I always carried two American Eagle coins. My naive American thinking was that they would carry more weight than traditional gold bullion on other countries. Today, I carry a one-ounce official Canadian Maple Leaf and a one-ounce South American Krugerrand. The gold value is the same as an American Eagle, but the representation of countries may be better received based on my location. I typically avoid pushing any American values during international travel, and attempt to appear more Canadian than American when visiting many countries.

You might consider lower weight coins, such as 1/4-ounce Krugerrands, but you will pay a higher price per ounce. You never want to expose these coins unless absolutely necessary during travel. This is why I hide them well. Small hidden pockets sewn into the interior of backpacks work well. If my international travel is successful, I will have no need to remove them, so I prefer them to be very hard to retrieve.

Another benefit of possessing gold while traveling is the ability to carry large value within small packages. If I stash \$35,000 worth of cash in my suitcase, this may raise eyebrows or trigger seizure of funds. A roll of ten gold coins has the same value, but appears less suspicious. It is also much easier to hide a roll of coins than a package of cash. If trying to be covert, placing bulk coins inside a standard paper bank coin roll can be convenient. The Canadian Maple Leaf coins are almost the exact same diameter as U.S. half dollars. A paper half-dollar roll discreetly hides 20 U.S. half-dollars or 18 gold one-ounce Maple Leaf coins. The label on the paper roll displays the value of the contents as \$10, and appears less suspicious. I often gift-wrap my coin rolls so that I can say they are a gift if questioned. One client only carries his gold coins within plastic collector's cases and explains that he is a coin dealer if questioned. Evaluate your own threat model and ability to explain your possessions before relying on these techniques.

Summary

Is all this effort really worth it? For me, absolutely. I value the privacy benefits of a truly anonymous home. For my clients under threat of physical danger, of course. Their lives may depend on absolute invisibility. For you...well only you can answer that. I will leave you with one final scenario to end this chapter. The following happened to a close friend and colleague two days before I wrote this section.

“Mary” returned from vacation to discover a concerning series of emails. An internet stranger, whom I will refer to as “Jack” had been attempting to reach her through her LinkedIn profile. Jack was selling a guitar on the mobile app LetGo and had been contacted by a potential buyer. The buyer sent a check to Jack for the purchase amount from a legitimate company with no ties to Mary. However, the “from” address on the FedEx shipment of the check included Mary’s full name and home address. It was made to appear that Mary was the person purchasing the guitar, and Jack now knew her full home details.

Jack assumed this was a scam, and suspected Mary may also be a victim. Mary assured Jack she knew nothing of this purchase, and Jack contacted the company identified on the check in order to confirm it was counterfeit. Mary may not technically be a victim, as she lost nothing, but her identity was used during the execution of a felony. The abuse of her name and home address as part of a scam bothered her. While not living completely anonymous, her operational security was strong, and she was much more private than the average person. She wanted to know why she was selected, and how the suspect found her home details.

When Mary contacted me to look into this, I did not suspect a traditional people search website. She is not listed in those, especially under her home address. Since I possess numerous data breaches as part of my online investigations service, I went straight for those. A search of her name, which is quite unique, led me to the HauteLook breach discovered in 2019. HauteLook had 28 million unique accounts breached in August of 2018, including full names, home addresses, genders, dates of birth, and password hashes. This data was sold in underground criminal communities. I confirmed that her full name and home address in the HauteLook breach matched the information provided about her on the FedEx label.

Mary had never heard of HauteLook, but confirmed the email address on file in the breach was her personal Yahoo account. I asked if she ever shopped at Nordstrom, which she confirmed. Nordstrom owns HauteLook, and HauteLook fulfills online orders placed through Nordstrom’s website. This was likely the connection. In other words, all of the details she provided for an order through Nordstrom were available to criminals, and likely being abused to make scam attempts seem more credible. There is nothing Mary can do to remove herself from this breached data. She can only change her habits from this point forward.

Her experience worsened a few days later. Mary received a \$4,000 invoice from FedEx demanding she pay the shipping fees for the numerous fraudulent shipments made in her name. The offender(s) created an account in Mary's name at FedEx, and opened a line of credit by providing her full name, address, and date of birth (all available in the HauteLook breach). This account was used to send multiple checks via overnight shipping without expense to the criminals. This was now full identity theft.

If she had used an alias name during her online orders, she would be less exposed. If she had the shipment sent to a CMRA or PO Box, her home address would not be abused. If she had done both, an internet stranger would not have been able to contact her. While his intentions were good, I see many internet victims which wrongly believe people such as Mary are part of the scam. I have investigated crimes where one victim attacked another, suspecting foul play. If we cannot be found, we have very little to worry about.

If she had established a credit freeze on herself, FedEx may have declined the line of credit in her name. A credit freeze is vital for all Americans, and I explain the entire process in a later chapter. I want to make it clear that I do not place fault on Mary. We have all made privacy mistakes, including myself. I recall the days where I ordered packages to my home in my real name. None of us have always executed the most private strategies. We all start somewhere. Will this encourage you to start being more private today?

International Considerations: Every day, someone contacts me about anonymous payment strategies outside of America. As a U.S. citizen, working in the U.S., and helping mostly American clients, I simply do not have much experience with masked payment services in other countries. If your country does not offer secondary credit cards or virtual options such as Privacy.com, I believe your best option is to possess a business credit card. Most international banks will issue cards in a business name for numerous "employees", and will only require the detailed information of the business owner (you). The bank will know every detail of each transaction, but the merchants which accept the card are shown only a business and employee name (alias). Please use the details presented here to create your own solutions. Some readers have reported that **Revolut** (revolut.com) offers virtual cards in alias names throughout Europe. However, this requires a premium account with a \$10 monthly fee.

I hope this chapter helps you dive into the world of anonymous payments. Once mastered, these strategies will prevent information leakage, and will keep you off various public people search websites. Remember, it only takes one mistake to unravel all of your efforts toward anonymity. Merchants have a financial motivation to share your information with other merchants and service providers. Marketing and advertising are more difficult thanks to our tendencies to skip commercials, block online ads, and refusal to answer telemarketing calls. Companies now rely on your data in order to make a buck. You can combat this with anonymous purchases, and by never associating your real name with your home address.

Typical Client Configuration

Private payment options are vital for my clients. The easiest way to unravel the efforts of achieving an anonymous home is to pay bills and make purchases with your true name. The following is my checklist for most clients.

- Possess enough cash to facilitate any daily purchases which accept it.
- Purchase prepaid gift cards for in-person purchases which refuse cash.
- Establish a Privacy.com account for masked online and in-person purchases.
- Obtain a secondary credit card for transactions which require a real credit card, such as a hotel visit or expensive online purchases.
- Establish a checking account in a trust name for utility payments.
- If desired, establish a checking account in an LLC name for utility payments.
- Establish all utility services in the name of a trust or LLC.
- Identify nearby Amazon Lockers and create accounts associated with these locations.
- If Amazon Lockers are not available, obtain an account at a local mail receiving agency which can accept packages in any name.
- If deliveries must be made to your home, conduct all transactions in an alias name with appropriate masked payment.
- When traveling, consider foreign currency, virtual currencies, and gold coins in the event of an emergency.

Overall, whenever possible, never provide a true name with any purchases.

CHAPTER TWELVE

EMPLOYMENT

Private employment is easy, as long as you are always paid in cash and never provide your name to your employer. If you are in this situation, your work is likely illegal, at least in the opinion of the IRS. There is no such thing as complete privacy in terms of employment in America, but there are several things we can do to minimize our exposure. This chapter will present many ideas, starting with the least private to the most. None of this is to avoid taxes or skirt financial institution reporting requirements. All of these tactics are legal, and only designed to provide privacy protection from the public. First, you should ask yourself if private employment is important to your overall privacy strategy. Consider the following.

In 1997, a woman who was a friend of mine from 5th grade tried to rekindle a friendship with me. I had not spoken to her in several years, and was not very close to her when we were children. Her initial attempt to contact me was through social engineering. She telephoned my grandfather (listed in the phonebook) late at night and insisted there was an emergency. She asked for my number (a landline), which was unpublished. My grandfather provided my number to my apartment and she began calling me daily. Her voicemails featured incoherent giggling and rambling, and it was obvious there was some mental instability. I ignored the calls.

Within a week, I started to receive voicemail messages from her on my pager (yes, I'm old). My grandfather did not have that number, as it was issued by the local police department where I was employed. I knew that the number was displayed on a call-out sheet which was widely distributed around the city. To this day, I have no idea who released the number, but it was likely another telephone attack. I continued to avoid the calls.

In the summer of 1997, I was working a patrol shift around 9 pm. I received a call for a holdup alarm at a local fast-food restaurant, which would be closing at that time. I raced to the scene and encountered this woman. She was an employee there, and pressed the alarm because she knew I would respond. My dispatcher had previously disclosed my shift and assignment to her over the telephone, after she identified herself as my sister. I called for another unit and she was charged with activating a false alarm. The arresting officer was a close friend of mine who had a heartfelt conversation with her about talking with a professional to seek help. She was later hospitalized with extreme schizophrenia. I do not know where she is today. My point with this story is that your fellow employees will fall for social engineering attacks. While trying to be helpful, they will disclose your home address, telephone number, work hours, and vacation times to anyone who has the talent to present a pretext or ruse. Anything you share with your employer is fair game, so let's choose how we provide sensitive details.

Traditional Employment

Let's start with traditional employment. When you apply for practically any job in America, you will be asked for your name, address, DOB, and SSN. Lately, some companies do not ask for an SSN until an offer of employment is made to you. My recommendation is to never provide an SSN unless an offer is made. If required on an application, I would enter "upon employment offer". This lets the potential employer know that you are willing to cooperate with tax reporting requirements, but do not want to provide your SSN when unnecessary. This prevents accidental exposure of your SSN when these applications are lost, leaked, or sold. They may require your SSN for a background screening, which is acceptable prior to employment if you feel the job offer will soon follow.

If you receive an offer of employment, you will be required to provide these details. This is likely for two reasons. First, most companies do a minimal background check through third-party services such as The Work Number, yet another Equifax product. Your potential employer will disclose all of the details you provided on the application, including your home address, to these services. Any information that a company did not already have about you, such as your new apartment address, will be added to your consumer profile and shared.

This is a very common way in which these data mining companies keep such accurate records on us. I would display concerning portions of Equifax's privacy policy here, but it does not matter. The 2017 breach of over 150 million people's full Equifax profiles eliminates any protections cited in their privacy policies. The data is now in the wild.

Second, your name, address, DOB, and SSN are required for legal payment, and will be included on an IRS form W-9. This allows the IRS to monitor your wages and ensure that you are reporting the proper taxes. I would have previously said that this data is private from public view, but the widely reported IRS breach in 2016 assures us this is not the case. Today, I can visit a handful of shady websites and query names from this breach. The free report displays full address history, and a small fee will provide me your DOB and SSN. There is no way to erase this damage.

This is a grim view to begin a chapter about employment privacy. However, I believe we have options to safeguard our information the best we can. First, I would never provide my home address on any application or W-9 form. This should only be your PO Box or UPS Box address. Your employer likely does not care much about where you live, unless the job has residency requirements, such as a police officer. The IRS does not object to the use of a mail box address. They just want their money. The majority of potential employers never require to know where you truly reside.

Next, I would have a credit freeze in place before submitting any application or tax form. This will be discussed later, but it basically locks down your credit from unauthorized queries. Companies such as Equifax can bypass this since they own the data. However, smaller companies that are hired to conduct background checks will not always be able to peer into your credit if you have a freeze in place. If you expect you will be releasing your SSN to unknown third parties during your job hunt and eventual employment, you must assume it will be handled carelessly. The credit freeze gives you major protections if and when a malicious actor stumbles across your DOB and SSN.

Once you are hired, there are likely to be more invasive requests. Many companies maintain a contact list of all employees which includes names, home addresses, personal telephone numbers, birthdays, and other unnecessary information. Expect these to be compromised and become public information. If pushed for a personal cell number, provide a MySudo or other VOIP number. If asked for a home address, insist on only displaying the PO Box or UPS Box previously provided. If questioned about this, claim you are moving very soon and will provide the new address once you have everything moved in. Conveniently forget to update this.

There are many careers where this does not work. Police officers, fire fighters, elected officials, and other government employees must disclose their true home addresses. This is usually to satisfy residency requirements set forth in outdated municipal laws. My first suggestion is to obey the residency requirement. If you must live within 20 miles of the police department where you work, meet this demand. Then explain your privacy concern to the proper personnel and request that your true address is not documented on any internal forms. This is a difficult task, and you may be met with great resistance. I know many people that have “shared” a low-cost vacant apartment in order to provide that address to their departments. I cannot recommend this. I can only say it has been done. If you are a public official, you have likely already given up much of your right to privacy.

My best advice for employees within traditional employment scenarios is to always challenge any privacy invasions. For many years, one of my clients accepted a condition of his employment at a police department which required him to purchase a landline telephone number and make it available to all employees of the city which he worked. When asked if he could provide a VOIP number instead, he was denied. After years of compliance, he asked to see the policy which enforced this annoyance. He discovered that a strict policy did not exist, and was allowed to terminate his landline and provide a VOIP number for daily abuse.

He then challenged the requirement to share his home address with all city employees. This led to a discovery that no policy ever existed for this demand. It was something everyone accepted without asking for details of the requirement. Today, he only provides a local PO Box address on the public roster. When you are faced with invasive demands from your employer, consider a polite request to learn more about the policies which enforce them.

Employee Identification Requirements

My first “real” job was at a local hospital. All employees were forced to wear employee credentials which included full name and a photograph. During my first day, a human resources representative captured my photo with a Polaroid camera, physically cut the photo to the appropriate size, and laminated it within my “name badge” while I witnessed the entire process. Things were much simpler back then, and I saw no privacy invasion with this mandate.

Today, things are much different. Many companies capture a digital photo with a dedicated employee identification system. The digital image is either stored internally at the company or shared to a third-party credential maintenance system. In either situation, leakage is possible. My bigger concern is the abuses which I have witnessed, such as the following.

- A technology-related company created Gravatar accounts for every employee’s email address and uploaded images to each. Every outgoing email now possesses the face of the employees served as an icon in the sender field. Since the company owns the domain, employees have no authority to modify or remove this image.
- A telecommunications company uploaded the photos of employees to their website and associated each with full names. Today, several archives are available to the public. These employees can never completely remove these images, as they have been scraped by dozens of archiving projects. Once on the internet, it is there forever.
- Another technology company forced all employees to participate in a Slack-style online communications platform. The company attached images of employees to the profiles, which were scraped by various online people search websites. Today, these public search sites display photos of the employees next to home address and telephone details.
- A police department shared the photos of all employees with the local newspaper. Today, whenever a police officer is mentioned in an investigation, the newspaper includes the photo of that person. The Associated Press has replicated many of the articles (and photos) nationwide. These photos are present on hundreds of websites which can never be removed.
- A financial company created caricatures of employees based on the identification photos and placed them online. Most images displayed enhancements of physical features that most would not want highlighted. These cartoon versions humiliated employees by magnifying big noses, acne, thick glasses, and in one unfortunate image a facial scar received after childhood physical abuse. These images were later posted to social networks by “friends” of the employees. The comments attached to the posts were crude and demeaning.

All of these scenarios happened without consent from the employees. This type of exposure may be outside of your threat model. However, I urge you to consider any future vulnerabilities. If you are ever charged with a crime or misdemeanor traffic offense, media outlets will try to find the most unflattering photo available. If a fellow employee becomes upset and seeks revenge against you, these photos can be abused on social networks and other online sites.

I recently had a client contact me after her head from her employee identification image was Photoshopped into pornography and posted online. We know that people can be cruel and there are endless ways to abuse digital images, but what can we do about it? Employers likely require images of employees, and the systems to store this data usually possess no security. I have no magic solutions, but I do offer a few considerations, in order of most advised to least.

- Have an honest discussion with your employer. Explain that you have specific reasons to protect your privacy, and you respectfully request that your image not be captured and stored by the company. Explain the vulnerabilities mentioned previously and identify how you may be negatively impacted by abuse of the images. If appropriate, cite any previous harassment or stalking issues which you have faced.
- Request to review any policies which require photographs of employees. Additionally, request details about the storage, sharing, ownership, and online publication of the images. You will likely find out that such policies do not exist. If they do, scrutinize them for loopholes. You will likely learn that nothing is done to protect the images from online attacks. You could ask to postpone any employee photos until the protection policies are in place. This may generate unwanted attention from your superiors, so approach cautiously.
- If appropriate, explain that you have a religious objection to captured images. Some have referenced the second of the ten commandments, which partially reads “Thou shalt not make unto thee any graven image or any likeness of anything”. A few denominations, such as the Amish and Old Order Mennonites, often refuse to have their photographs taken due to this wording. Expect eye-rolls if you go this route. You may become known as a difficult employee which could cause other issues. Always choose your battles wisely.

As a new employee, you may not want to become too forceful with your requests. Please consider any consequences before execution. Seasoned employees may have an easier time refusing employee photos as they may possess more job security. I present this section simply to create awareness of the issues surrounding employee photos. Your results may vary.

Company Parking Permits

In 2019, I began witnessing a new privacy invasion from employers. Businesses began demanding full vehicle details of every employee, all of which are commonly stored within a third-party verification system, and of course shared with other companies. In 2020, the make, model, color, VIN, registration, and insurance details were requested from one of my clients. She had conducted a full privacy reboot and did not want her vehicle associated with her true name. When she questioned the necessity of these details, the employer only stated it was a new policy. We later discovered that the details were being provided to a third-party parking management company. The employer had outsourced the parking garage to another business. The parking company which requested the details of my client's vehicle also associates the following information to the employee's profile.

- Date and time of each entry into the garage (When she arrives to work)
- Date and time of each exit from the garage (When she leaves work)
- Length of stay (The number of hours she worked)
- Average length of stay (The average hours she works)
- Daily average length of stay (The days she works less than others)
- Photograph of each entry (A daily image of her driving the vehicle)
- Photograph of each exit (Another daily image of her driving the vehicle)
- OCR text of the license plate (Searchable log of all usage by her vehicle)

To add insult to injury, the privacy policy of this provider clearly states that they can share or sell any information with any third parties solely at their discretion. Similar to the previous section, there are no fool-proof strategies to prevent the collection of these details. Most of these scenarios include a physical parking permit which grants access to the parking areas. The details of the vehicle are not necessary in order to enter the parking areas, but usually gathered for record keeping. My client informed her employer that she was currently driving a rental vehicle and would disclose her true vehicle information once she received it back from repair. She "forgot" to update the record and continued to park her true vehicle in the garage without any repercussion. However, a few months later, the company again demanded the details of her vehicle. The next day, she arrived to work in a rental vehicle and provided the make, model, color, VIN, and registration. Her employer was content and shared the details with the parking company. She returned the rental and continued using her true vehicle the next day. She cannot prevent the system from tracking the usage of her parking pass or capturing images of her activity. However, the system does not have any record of her VIN or registration. This protects the identity of the owner of the vehicle. Her magnetic plates, as previously explained, are removed the moment she leaves the public roadway and enters the private property of her employer. This is legal, as there are no vehicle registration requirements on private property. Is this overkill? Probably. However, she enjoys the rebellion, and benefits of privacy.

Final Employee Considerations

Many careers require a government license. These include hair stylists, Ham radio operators, nurses, veterinarians, and many other professions. The details of these licenses are public record. If you are skeptical, navigate to www.myfloridalicense.com/wl11.asp and type in any generic name. The results include full license details such as name, home address, telephone number, license acquisition date, expiration, and profession. If you require a specific license for your employment, only provide a PO Box, VOIP telephone number, and burner email address. This information will be abused.

Some careers have more exposure than others. I am consistently contacted by celebrities and politicians seeking more privacy. While I can provide anonymous lodging and alias payment sources, I cannot remove them from the spotlight. There is nothing I can do to make Tom Hanks completely invisible (but I am willing to try if he should call me). You should consider the overall exposure of the type of employment you are seeking. If you have a public presence, you risk exposure in newspapers or the local television news. If you work for a private company inside of a building all day, your risk is minimal. Most of my clients just want to fade into the background with the most minimal amount of attention possible. Overall, traditional employment will always expose your name, DOB, and SSN. In most scenarios, you can keep your home address and cellular number private. The rule is to always assume that any details provided at any time during the employment process will become public information. If we go in with this attitude, any damaging exposure should be minimal.

Consider a few more tips in regard to working inside an employer-owned building. Much of this may seem redundant from Chapter Three. Previously, I explained ways to protect yourself digitally while in your own home and within spaces which you have control. When at work, you are much more vulnerable. I believe you are more prone to eavesdropping attacks. The following is a short list of tactics which should be executed while at work.

- Cover webcams on any employer-owned computers and mobile devices.
- Insert microphone plugs into employer-owned computers and mobile devices.
- Never use personal devices for work-related tasks and vice versa.
- Never use your work email for personal communication and vice versa.
- Never use your work cell phone for personal communication and vice versa.
- Never connect to personal email accounts from employer networks or computers.
- Never connect personal devices to employer-provided Wi-Fi or Bluetooth.
- Never connect personal devices to USB ports of employer-owned computers.
- Faraday bags should be used for personal devices to block wireless scanning in offices.
- Refrain from sharing details of your employment within social networks (LinkedIn).
- Request your birthday (DOB) be eliminated from celebratory email blasts.

Self-Employment

Contrary to traditional employment, self-employment can provide many advantages in regard to privacy and digital security. If done properly, you will never need to disclose your DOB, SSN, or home address to any entity. You can be paid through an LLC which possesses a valid EIN from the IRS, which is much more private with less risk of public exposure. Your first task would be to identify the type of work you desire.

There are countless career choices for the self-employed, and I am not here to guide you into any specific direction. I have had clients who possessed their own home-based businesses, conducted on-site training and consulting, and ran various online stores. Only you can decide what type of business fits best with your personality and experience. My goal is to guide you through the process of making your choice legal and private.

Your first task is to establish the legal infrastructure for your business. This was previously discussed as a privacy tactic for asset ownership. The process for establishing a business which anticipates income is very similar. The LLC documents previously mentioned can be used for your new venture. However, there are many considerations for the public filing of your new business.

During the previous legal infrastructure chapter, the goal was complete privacy. I discussed the New Mexico LLC which could shield the true owner of an LLC from public view. In my opinion, this level of privacy is not vital for a business which will be used to generate income. You will be required to disclose your true identity to the IRS and any financial institution which you use for payments and distributions. If you will be conducting any type of consultation, training, or other services, your name is likely to be associated with the business in some form. Therefore, I don't strive to hide the identity of the owner of a business.

The first step is to establish your LLC in the state which you reside. For a small number of readers, that may be the state where you established nomad domicile, such as South Dakota. For most of you, it will be the state where you own a home or possess a driver's license. Every state has their own rules, and you should spend some time reviewing the state's business entities website. There are also many local businesses which will assist you with establishing the LLC (at a substantial cost). If you have made it this far into the book, I have no doubt that you can do this yourself.

At a minimum, the state will want your name, address, email address, and telephone number. The address you provide can be a PO Box or UPS Box, the email can be a ProtonMail account designed specifically for business use, and the telephone number can be any VOIP service you use. As with the previous lessons, everything you provide will become public record.

Nomad Business Registration

In order to possess extreme privacy, you might consider the nomad residency route discussed earlier. If you do, you have the ability to legally establish a publicly invisible LLC which can be used to generate income. The IRS will know you are connected, but this method provides many privacy strategies unavailable to traditional employment. The following scenario assumes you are a legal nomad resident of South Dakota and you possess a PMB and government identification from that state. I explain other options afterward.

The first task is to choose the name of your new LLC. This needs to be something that is not already in use in the state. I prefer generic names which could describe anything such as Ventures Unlimited LLC or Consulting Group LLC. Conduct a search at the following website. While you are there, take a look at a typical completed application, which is visible on the business details page.

<https://sosenterprise.sd.gov/BusinessServices/Business/FilingSearch.aspx>

Next, you should decide which address you will use for the LLC. While you could use the South Dakota address provided by your personal PMB provider, you may choose another option. For extreme privacy, I prefer to use a unique address for my business. This creates another layer of privacy and does not expose my “home” address publicly. Similar to the New Mexico example in a previous chapter, a South Dakota LLC requires you to possess a registered agent within the state. For most clients, I use Americas Mailbox as the business PMB, just as I did for the personal ghost address. I am reluctant to promote Americas Mailbox for nomad business registration, but I don’t have any better options. I have had several problems with their service over the years. Missing mail has been an issue and their customer support staff are rarely helpful. On one occasion, I received an LLC renewal reminder from the state five months after it arrived. However, their new scanning feature allows me to cautiously approach their service again for this purpose.

The procedure for establishing a business PMB at Americas Mailbox is the same as previously mentioned. If you are combining your personal and business PMB usage, you only need one address. This is what I do for most clients. Be sure to select the scanning feature and the registered agent service when you create the account. This will add a minimal fee to your annual plan, but will keep you legal with the state. Contact the service and ask which name you should provide as your registered agent. You will need that for the state application process. You will be required to submit a USPS form confirming your identity as previously explained. You can use your America’s Mailbox address on this form. Be sure to list your LLC name as a confirmed recipient on this form. I also include my Contract Officer’s name, as explained momentarily.

Once you have confirmed your PMB with registered agent service, the next task is to apply for an LLC with the state. This is done online, and the result is immediate. In previous years, applications required physically mailing the documents and waiting for a confirmation. The entire process now takes less than ten minutes. This is extremely beneficial. Some states, such as Washington, require months of processing before an LLC is approved. Navigate to <https://sosenterprise.sd.gov/BusinessServices/Business/RegistrationInstr.aspx>. The site will walk you through the process, prompting you to make decisions along the way. Avoid completing any “optional” fields. The application process is split into twelve categories. The following provides notes on each.

- **Business Name:** The name you selected after confirming it has not been taken.
- **Addresses:** Any address information should be your new PMB.
- **Agent:** Select the “Non-Commercial” option and enter the name of your agent provided by your PMB. Conduct a search and choose the appropriate option.
- **Organizer(s):** You can select an individual or a company for this. South Dakota allows you to specify your own LLC as the organizer, which I find interesting. If you would rather assign an individual, you can add your own name or another “nominee”. I have a close friend with a very generic name such as John Wilson. I pay him a small annual fee to be my “Contract Officer”, and he has the authority to “Organize” my business. His address is not required.
- **Detail:** Choose “Perpetual” in order to set no specific expiration date.
- **Manager(s):** Select the “Member-Managed” option and “No”.
- **Beneficial Owner(s):** Optional field to be avoided.
- **Additional Articles:** Optional field to be avoided.
- **Recipient:** Optional field to be avoided.
- **Confirmation:** Make sure everything looks right.
- **Signature:** This is a digital input and no “wet” signature is required. The name you provide will be public record. I ask my Contract Officer to be the authorized signee.
- **Payment:** You can pay with a credit card, prepaid card, or Privacy.com card, depending on your desired level of privacy.

After successful payment, you will immediately receive a digital copy of your Articles of Organization and Certificate of Organization. You now possess an official and legal LLC in the state of South Dakota. If you are not a nomad in that state, you should consider creating an LLC within the state of your residence (or domicile). The steps should be similar, but each state possesses its own nuances. Some states can be very invasive and demand to know the full details of LLC ownership. If using the LLC for income, this is not a huge concern, as the business will be associated with you anyhow. My only mandate would be to never disclose your true physical address within any registration documents. It will become online public information within days.

Traditional Business Registration

I assume that most readers are not nomads of South Dakota. Those readers might need to create an LLC in their own state in order to possess the privacy protection which are explained in a moment. I cannot explain the LLC creation process for every state, but I can offer some general guidance.

- Income-aggressive states such as California demand \$800 per year for every LLC registered within the state. This is regardless of income. It also demands full ownership of the LLC be publicly available online. For most California residents, I do not recommend an LLC for self-employment. The Sole Proprietor option will be explained momentarily.
- Nomads who want to conduct business within income-aggressive states must register the company as a “Foreign LLC” within the state. This is usually not required for online businesses, but if you plan to step foot within California during the course of your business, expect to pay them their share. Failure to do so will result in numerous penalties and additional fees.
- Once you register your LLC, you are likely responsible for annual renewals and tax reporting within that state. Even if you make no income, you may be required to disclose that within an annual tax return. Failure to do so can result in financial penalties and termination of the LLC.
- Any time you register your LLC through a third-party service, such as Dun & Bradstreet (D&B) or various U.S. government portals, you risk online exposure. When possible, avoid these services. When forced to apply, provide details which can become public without much concern.
- If you have registered an LLC with the state and have no intention to use it in the future, you should file a request to legally “dissolve” the company. This prevents annual reporting after the final year of operation.
- Revisit the information about the Corporate Transparency Act which I previously explained. Most states are going to demand to know the true owners of an LLC and will pass this on to the federal government. I do not find this to be a problem, as we will register our LLC’s with the IRS for use during self-employment. Remember that an LLC used for income is never intended to be “anonymous”.

If maintaining an LLC with your state while meeting all documentation, regulation, and tax reporting requirements seems overwhelming, consider becoming a Sole Proprietor, as explained next. It provides less liability protection than an LLC (which is currently minimal for sole member companies anyway), but can be accomplished with minimal effort.

Sole Proprietorship

Self-employed people who possess an LLC with EIN have some great privacy protections. Instead of providing a personal name and SSN to customers, they can supply the LLC name and EIN. This is not limited to official LLCs. Any individual can conduct business as a sole proprietor and provide a fictitious “Doing Business As” (DBA) name. You can also obtain an EIN without the need to pay annual LLC fees within aggressive states. Before I explain the process, let’s define the typical reader who may want to conduct business as a sole proprietor.

- You are a self-employed individual (not a partnership).
- You do not have any employees.
- You do not want to provide your name and SSN when conducting business.
- You want to be paid in the name of a business.
- You want to open a banking account in the business name.
- You want to avoid annual LLC fees and filing requirements.
- You desire simplicity within your self-employed strategy.

If ALL of these apply to you, a sole proprietorship may be ideal. In most states, government documentation is not required in order to be a sole proprietor. Any individual can simply claim to be self-employed with this status. The IRS does not demand filing, as your income can pass through your individual tax return. However, those becoming a sole proprietor for privacy reasons must take additional steps.

First, you should choose a business name. In most states, you may use your own given name or an assumed business or trade name. Choose a business name which is not similar to another registered business. Conduct a search within your state’s corporation registry website and with your local county clerk’s office. After you have picked a name, such as “Privacy Solution Services”, you must file an “Assumed” or “Fictitious” business name registration with your state. This can usually be completed within your local county’s offices and will require a small fee. Finally, you should obtain an Employer Identification Number (EIN) from the IRS, as explained next. This is not a federal requirement, but will be necessary for our needs.

You can now operate under the name of your business without the need to possess a complicated LLC. Your official business might be something similar to “Michael Bazzell, DBA Privacy Solution Services”, but you can identify yourself to customers simply as “Privacy Solution Services”. With an EIN, you can open a banking account with this name and print only the business name on checks. You can provide the EIN instead of your SSN to customers. Note that you possess no liability protection as a sole proprietor, but the protections to single member LLCs are weak anyway. This is the easiest privacy strategy to protect your name and SSN as a self-employed individual. Contact your state for full details.

IRS Registration (EIN)

If you plan to ever generate income in the name of the LLC or sole proprietorship, or open a business checking account, you will need an EIN from the IRS. You can bypass this if you plan to funnel income directly through your own SSN, but that defeats the point of the business as the wall between your identity and your income. Obtaining an EIN is simple and immediate at <https://sa.irs.gov/modiein/individual/index.jsp>.

You can complete the application any time from Monday through Friday, 7 a.m. to 10 p.m. Eastern Time. The process will demand your full name, address (PMB), and SSN. There is no legal way to facilitate an EIN without making this connection. Fortunately, this data will not be (intentionally) released to the public. I believe an EIN is vital for private employment. It allows me to truly segregate my personal information from the various public disclosures that are associated with accepting payment. Every time a client or customer requires a tax form, I can keep my SSN private. If I need to complete registration through a third-party vendor, my name can stay out of most paperwork and invoicing. Most importantly, I can now create a business checking account for deposits and payments. This new account can continue the public isolation from my true identity.

Business Bank Accounts

Banks in America must follow strict government regulation in terms of opening new accounts. “Know Your Customer”, alternatively known as know your client or simply KYC, is the process of a business verifying the identity of its clients and assessing potential risks of illegal intentions for the business relationship. If you wish to open a new bank account in your business name, you simply must disclose your true identity and association. Consistent with previous instruction, I always recommend seeking locally-owned banks and credit unions instead of large chains. They will have less requirements and offer better privacy. When you open a new account under an LLC, you will need the following.

Government Identification
LLC Articles of Organization

LLC Certificate of Organization
IRS EIN Confirmation

In rare scenarios, they may wish to view your LLC Operating Agreement. I have allowed this, but I do not allow a copy to be made. This agreement contains sensitive details such as your shares of the company and specific organization of members (if applicable). As long as you are forthright with your true name and proof of PMB address, you should have no issues opening a new account. You will be asked for a deposit into the account, which then allows you to use typical checking features. As before, I always request as many “temporary” checks as the institution will allow upon creating the account. I also request that a mailing address is absent and that only the business name appears on them.

Credit Card Processing

In my experience, many potential clients or customers will want to pay you with credit cards. This can be very simple with popular privacy abusers such as PayPal, but I never recommend them. PayPal currently shares your data with over 600 third-party companies, and appears amateur on an invoice. Instead, consider better options. I recommend Stripe or Square for all credit card processing. They are not perfect solutions, but they possess much cleaner privacy policies than PayPal or other payment collection options.

Stripe will require your full name, SSN, DOB, business name, and EIN. This is required per the KYC demands as previously mentioned. Once you are approved, you can insist on the EIN receiving the tax forms (if required). The true power of Stripe is the ability to embed its software into your website, but that is probably overkill for most small business owners. Most of my clients who own small businesses simply send electronic invoices straight from the Stripe dashboard on their website. The recipient can pay via any credit card, and you receive the funds within a couple of days. Stripe will want to know where the funds should be deposited, and I recommend the business checking account previously mentioned.

Square is almost identical in regard to account creation requirements. The additional benefit of Square is that they will issue you a credit card reader, which allows you to physically accept credit cards through any mobile device. Both options will charge you a fee of approximately 3% of each transaction.

Virtual Currency

As previously stated, cryptocurrencies such as Bitcoin can provide a great layer of anonymity. If you provide a service of interest to those in the virtual currency world, you should be prepared to accept Bitcoin. Use the techniques previously discussed to create and configure your own Bitcoin wallet. Advertise that you accept Bitcoin, either through a website or in the physical world. Consider my adoption of Bitcoin.

From 2013 through 2020, I offered online training courses. 99% of the purchases were made with a credit card on my site through Stripe. However, I also advertised that I accepted Bitcoin. Over those years, I slowly built a wallet full of Bitcoin without the need to create an account through an exchange. I now have funding in this wallet to pay for various online services. I still needed the credit card transactions in order to keep my business afloat, but the incoming Bitcoin provided a strategy to obtain it anonymously.

Contractor Considerations

When you begin conducting business with larger organizations, you will find many of them have their own vendor registration requirements. These can be a deal-breaker for me. Some are minimal and only require the information that you have already made public via the steps previously mentioned. However, some are extremely invasive, and I will present a few scenarios here.

Overall, government vendor portals are the worst privacy offenders. In 2012, I was hired to teach a course for a military organization. They required me to be registered in the General Services Administration System for Award Management (GSA SAM) website at SAM.gov in order to receive payment. I was naive and assumed that my data would be protected. I provided my full name, actual physical address, and my personal email account. This became public data and was immediately shared with hundreds of other businesses. I began receiving unsolicited offers to help grow my business and learn how to navigate federal contracts (for a fee, of course). Today, I still receive email from these outfits, even after I completely removed my registration.

Many companies will require you to be registered in the Dun & Bradstreet (D&B) database in order to collect payment for services. This private organization has somehow become the minimum standard requirement for private and government contracts. At least once a month, we must turn down a potential client because they demand we share our data with D&B. While their privacy policy is riddled with concern, a single paragraph sums it up:

“Dun & Bradstreet shares information with third-party service providers, such as credit card processors, auditors, attorneys, consultants, live help/chat providers and contractors, in order to support Dun & Bradstreet’s Internet websites and business operations...We may also disclose the information as required or appropriate in order to protect our website, business operations or legal rights, or in connection with a sale or merger involving Dun & Bradstreet assets or businesses...From time to time, Dun & Bradstreet compiles online and offline transaction and registration information for internal analyses, such as market research, quality assurance, customer experience, and operational benchmarking initiatives.”

In other words, they can share your details with anyone. Even worse, D&B has already had one known breach that exposed the profiles of over 33 million businesses and owners. Why should this matter when the business details are already public? The reason is that D&B requires much more invasive information in order to have the privilege of them selling your data. This includes the following.

- Full name of owner (not just the business name)
- Physical address of owner (no PO or PMB allowed)
- Telephone number (no VOIP allowed)
- Employee details

I applied for, and received, a DUNS number from D&B in 2013. During a regular reminder in 2016 to verify my company information, I was prompted to enter a valid physical address. I had my PMB on file, which was now being rejected. I attempted to enter a handful of business addresses, all of which were denied. Without my true home address, I could no longer possess a valid registration. I happily deleted my profile, and I have not had one since.

Local municipalities are also reckless with your information. In 2015, I was contracted by the city of Reno to conduct an OSINT training course. The course was canceled after they could not locate a venue, but the contract was published to their website. It displayed my name, PMB, full details of the event, and my signature. I had to make several requests to redact my address and signature. After much hesitation, they finally modified the online document. Again, you must assume that every detail provided to a client will be made public.

The purpose of a private business entity is to shield you from personal data exposure. If you have created your own LLC properly, you are prepared to conduct legal business and accept payment while never disclosing personal information. Consider the following typical invasive procedures, each of which include the public information which you can provide without risk.

W-9 Form: As a sole member LLC, or partnership LLC, companies are required to submit proper tax reporting to the IRS if you are paid more than \$600 yearly. Legitimate companies will require you to submit an IRS W-9 form. You only need to disclose your business name, EIN from the IRS, PMB address, and an illegible signature. The IRS can later verify your actual income with your reported earnings. Your name does not need to appear on the W-9 itself, as the EIN is associated with your SSN behind the scenes.

Vendor Paperwork: If you conduct work for large organizations, they will demand you be entered into their third-party vendor systems. These are notorious for leaking details into public records. You can provide only the business name, PMB address, business ProtonMail email account, burner telephone number, and IRS EIN. If they insist on a contact name and signature, you can appoint anyone as a nominee for this. My good friend with the extremely generic name mentioned earlier is paid a very small annual fee to be the official contact and signature on many of my contracts. He is my “Contracting Officer” and often serves as the public face (name) within any publicly exposed documents.

Payment Records: Many government entities are required to publicly disclose all payments to third parties. You may see these notices on local newspapers or on websites. This data is collected and aggregated by various data mining companies. When this happens, I prefer my LLC to be listed instead of my name. Your LLC prevents personal exposure.

The weakest link here is the IRS. They can connect you to your LLC through the EIN. I do not see this as a threat for most people. I would much rather provide my EIN to strangers than my SSN. Hiding my SSN protects me from rampant tax return fraud. Supplying a business name instead of my real name to business clients prevents an easy lookup on various people search sites. When the details of my business become public, my name is not present on the vendor forms.

If you possess a nomad residency and South Dakota LLC, you can safely share business details and remain private. The address provided within the various documents required by your customers is not a risk. It displays a physical address you have never visited. That PMB service does not know where you live. The EIN provided cannot be abused as much as an SSN. A DOB should never be required, and the creation date of the LLC can be provided when demanded. You possess a great shield that protects your personal information.

This may all seem invasive for a book about extreme privacy. Remember, this LLC is only required if you plan to generate income under a business name and do not want to publicly disclose your personal details. In order to better explain how all of these steps can help us achieve better privacy and security, please consider the following true scenarios from my own LLC experiences.

- I was asked to submit a W-9 in order to be paid for an on-site consultation. My W-9 displays my business name, business PMB, and EIN. My name and SSN do not appear. This is now kept on file at an accounting desk which likely possesses minimal security. If it leaks, I really do not mind. The PMB address is not my personal PMB address, and I have never physically been inside either.
- A government entity publicly posted all payments on their website. My business name and the amount I was paid is present today. Searching my name will never reveal this information. Searching the name of the LLC reveals my organizer, but not me. One would need to connect all of these details together in order to identify the payments made to me, which is not possible with publicly-available information.
- A company required me to comply with their vendor registration demands. The data provided was shared with an employment verification service and added to their own database. Neither system possesses my name, SSN, DOB, or personal address. The data being shared and re-sold does not compromise me personally.

- I needed to make a payment from my business checking account. I do not possess a credit card in the LLC name. I created a Privacy.com account and associated it with my business checking. I now use masked debit card numbers to make purchases without risk of personal exposure.
- I presented a keynote at a large conference. My speaking agency only supplied my business details and contact information during my registration. A complete roster of all attendees and presenters was given away, including names, home addresses, telephone numbers, email addresses, and social network profiles. My entry contained no sensitive details and I have no personal exposure.
- I provided training at a BlackHat event in Las Vegas. Only my business details were given for payment, which were eventually shared with all the vendors at the event. My name was not present on any of the promotional instructor details. The address provided is a mail drop with no public association to me. The email account provided was a masked service which I disabled immediately after payment. I now receive no unsolicited communication about the event.
- The state where I registered my LLC knows the business name, but not my name. The address on file is a PMB with no public association to me. Searching my name within the state website reveals no records. Searching my business name does not reveal my name or personal PMB address. I have isolation between my personal and business details.
- The IRS knows my true name and that I own the business. The addresses on file are both PMBs. This data is not (intentionally) public, but would not be damaging if a breach or leak occurred. Identity theft criminals usually focus on personal tax profiles instead of business filings.
- My bank and credit card processors know my true name and that I own the business. They do not know a true physical address for me nor my personal PMB address. A search warrant to multiple organizations would be required to expose the relationship. This is extremely unlikely and outside of my threat model.

I openly provide my accountant with all income, expenses, and tax documents. I legally comply with all state and federal tax reporting requirements. The IRS takes their share and is happy. The state in which I physically reside gets its cut when I file my state tax return, using a local PO Box as my physical address. I obey all tax laws and have no fear of an audit.

Whether you choose traditional employment or decide to become self-employed, there are many privacy strategies ready for you. You must be diligent whenever personal details are requested. Always expect that any information provided to governments or clients will become publicly available and permanently archived online.

Data Protection

I offer one final consideration for those who decide to become self-employed. It is extremely likely that you will need to store data about your customers. While online cloud-based storage is convenient, it is risky. Please apply the same privacy and security protocols toward your clients which you would demand yourself. This is not only ethical; it may save you from a lawsuit.

We hear about data breaches every day. Months later, we hear about large financial settlements to the victims (customers) of these attacks. Assume that anything you place online could be copied, stolen, traded, and sold. This can be devastating for your business's reputation (and bank account).

My company never stores any customer data online. This includes contracts, waivers, and custom strategies. Documents are sent securely through E2EE communications services with ephemeral expiration enabled, and deleted immediately from the service after receipt. Every customer is assigned their own VeraCrypt container stored on an internal server located on-premises, which is protected by a unique password. An employee cannot access this data unless authorized with the password assigned to their client. This container never touches the internet and is never copied to another computer. If this container would accidentally or intentionally leak online, it would be useless data without the password. If a client requests removal of all data about them, we can simply delete the container and purge it from our on-site backups without accessing the content.

This strategy is not only designed for the benefit of the client, but it also protects me from dealing with data breaches. I would never consider an online server, virtual cloud server, Amazon bucket, OneDrive account, Google Drive system, or Dropbox-style solution for the sensitive content trusted to me by my clients. I ask you to consider the same.

Summary

Every employment situation is unique, and I have no typical client configuration to present to you. Please use the strategies presented here as an initial guide toward creating your own employment playbook.

CHAPTER THIRTEEN

PETS

My dog has two aliases. Please continue reading and let me explain before you dismiss this chapter as pure paranoia. My German Shepherd is named Riley. His aliases include Kosmo and Lightning. Surprisingly, obtaining and maintaining a pet anonymously takes a lot of effort. Paying cash to a home-based puppy breeder is easy, but every pet related encounter past the original purchase is extremely invasive. The shelters offering rescued pets are funded by pet marketing companies, veterinarians, and pet supply organizations. Many counties share vaccination records with third parties. In all of these scenarios, your personal information as a pet owner is valuable, and abused.

In 2018, I had a client who completed my entire program and possessed a completely invisible home. She had no connection from her real name to her home or the area where she lived. She was running from an extremely abusive person, and her ability to live safely required her to stay off radar completely. After settling in, she wanted to adopt a dog from the local shelter. Since the shelter was constantly pushing dogs and always overcrowded, she assumed this would be an easy task to complete anonymously. She showed up, looked around, and fell in love with a young mixed-breed dog. She played a bit, went for a walk, and was determined to take the dog home that day. She approached an employee at the shelter and shared her intent. The employee handed her an application for adoption, and it all went downhill quickly.

Obviously, the application wanted a full name, address, telephone number, and all other basic details. My client was a pro with this, and had an alias name ready to go. However, she was immediately stopped in her tracks. The shelter demanded to view, photocopy and maintain the copy of her state issued identification. Furthermore, they reserved the right to visit the home for an inspection. The final nail in the coffin was demanding the right to share all submitted details with third parties including pet insurance companies, lost pet services, and social networks. She was a bit devastated. She left alone without a companion, and contacted me requesting assistance. The following details may be received with anger or skepticism. As an animal owner and advocate for adoption from shelters, I stand by my actions. As long as the animal is given a loving home, I have no objection to bending the rules a bit in order to maintain privacy. You will learn how standard pet adoption with your real information populates public databases within months and exposes your details for the world to collect.

My client lived in a popular urban area, and I had a meeting with another person in that area when this client reached out about this problem. I was able to meet this client at the shelter in order to get a feel for the operation. It was similar to every other animal shelter I had seen,

and was very similar to the shelter from which I obtained Riley. It possessed overworked and caring staff with strict rules in order to prevent animals from going to abusive homes. I obtained an adoption application and confirmed everything my client had told me. The shelter was on top of their game.

I walked around, played the role of a potential customer, and made small talk with a handful of employees. I executed the best social engineering attempts of my capability, and struck out non-stop. I failed with each of these pretexts.

“I really value my privacy, and I simply do not want to provide a copy of my license. I am open to a home visit, but I have been the victim of identity theft several times and refuse to add to that mess.”

“I am a full time Canadian citizen, so I only have a passport. It is illegal to copy a Canadian passport. Can I offer anything else?”

“I don’t drive, and have not had a state ID for many years. What else can I show you? A utility bill or cell phone statement?”

There was no budging. If I could not provide government identification and proof of residency, they would not release an animal to me. If I refused to sign the waiver to share data with third parties, I could not adopt a pet. This is actually very common, and I was not surprised. My client and I left the shelter and began discussing our strategy.

At first, my client was open to just releasing her real name and address, and trusting that it would not be made public. After all, who would an animal shelter give the data to that would have any real impact? You might be surprised. This shelter released the entire application to the following organizations, which then used the data as explained.

24PetWatch: This service provides a free portal for shelters to use for microchip identification. When the shelter gives you the animal, they update the microchip pet record with services such as 24PetWatch. For the shelter, this is a great deal. They get free microchips, readers, and the ability to update records nationally. However, 24PetWatch gets even more benefit. They get your personal details and the pet information. This is then used for marketing, as 24PetWatch offers many premium services such as pet insurance. Should you care that services like these have your name and home address? Let’s take a look at excerpts from their privacy policy:

- “By registering as a user with 24PetWatch you consent to Pethealth Inc., its subsidiaries, affiliates, trademarks, brands, and partners contacting you and collecting,

- using and disclosing your personal information for its own use and/or to any of our service providers.”
- “We may need to disclose the personal information we collect to affiliates, subsidiaries, partners, successors and other service providers or agents who perform various functions for us.”
- “We may also use this personal information to assess your future needs and to offer the products and services selected by us that may best meet those needs, from affiliates, reputable organizations with which we have strategic alliances or ourselves.”

In other words, they can share, trade, or sell your details to any company or outfit they choose. This can then make its way to data breaches and marketing databases. Eventually, you can expect to see your details within data mining companies and people search websites.

Local Veterinarians: Most shelters have relationships with local veterinarians. These relationships help the shelters obtain services such as spaying and neutering at a severely discounted rate, if not free. In return, shelters often share all of the adoption details with the vets in order for the vets to obtain new customers. The result is often unsolicited mail to the name and address on file and occasional sharing of this data with third-party affiliates. In this case, one vet automatically enrolls you with their patient portal VetScene.

VetScene: This is a portal often used by veterinarians in order to have better communications with their patients. Ultimately, it is a way to bombard you with mailed offers of premium services and reminders of upcoming appointments. The fees to VetScene from the veterinarian are often justified due to the influx of new money spent on services and otherwise avoided vaccines and appointments. Their privacy policy contained the usual suspects, such as implied consent to share all details with third parties.

I hope that you are now convinced that providing your personal information to an animal shelter will definitely expose you to numerous third-party data companies. This may be acceptable to you, and I hold no judgement. Since you have made it this far in the book, I must assume that you do not want to consent to this exposure. In order to protect the identity and location of my client, we executed the following strategy.

The first step was to volunteer. When I requested the adoption application, I also requested a volunteer application. Since most shelters are desperate for volunteers, they do not always scrutinize these applications. While the shelter definitely wanted the same details as for an adoption, they did not demand identification to volunteer. My client completed the volunteer application with her alias name and real address, and provided a VOIP burner telephone number as a contact option. She gave the completed application to the shelter and scheduled her volunteer training session for the following week.

She began volunteering twice weekly at the shelter. She walked dogs, helped at public events, and most importantly made friends with the staff. The relationships she started to foster turned her from a potential customer to a friendly volunteer who could be trusted. The dog that she wanted had already been adopted, but this gave her an opportunity to learn more about the shelter, their privacy policies, and be around numerous potential lifelong pets.

Three weeks into her volunteer journey, the original dog that she wanted was returned to the shelter. The family that adopted it could not tolerate the energy and was not able to provide the patience and discipline required to raise a happy dog. My client contacted me right away and said she wanted to jump on the opportunity. She admitted that she did not possess any friendships that would waive the adoption requirements, but that she was a trusted volunteer. Since this shelter was always full, I advised her to offer to foster the animal. Many shelters will happily send animals home with fosters in order to free space in cramped shelters. They usually provide food, kennels, and toys.

She drove back to the shelter and commented to a head employee that the place seemed more crowded than usual. She then asked what happens when they have no room for more animals. The employee explained the foster program and advised that they would reach out to fosters on file and beg for help. My client jumped on that opening and stated that she desired to be a foster. Of course, there was another application for that, but the employee did not ask for ID since my client was a registered volunteer with a record on file at the shelter. My client took her future dog home that day.

This was a big achievement. The dog was in her house. The shelter only knows my client by an alias name, and they know her true address. I advised her to do her job for a few days, enjoy the bonding, and ensure that the dog was a good fit. During her next volunteer assignment on a weekend when specific staff were present (the staff that she had bonded with the most), she advised them that she would like to adopt the dog she was fostering. This immediately presented the adoption application, which she completed with her alias name. The employee asked for an ID, which my client stated "I don't have it today, but I can bring it on Tuesday when we go to the Adoption Event". This was fine with the employee, and the rest of the application was executed. My client now owned the dog. At the next volunteer event, which was located at a local pet supply chain, the day was too busy for anyone to remember to obtain a copy of her ID. To this day, she still volunteers at the shelter, and no one has ever mentioned a need to copy her ID.

You may be reading this in disgust. I have encouraged a client to lie to an animal shelter. I can only offer the following. She hurt no one. She is an amazing and loving dog owner. Without the ability to stay private, she would not have obtained a pet from a shelter. Her actions were not in vain. The following events have occurred to her since the adoption.

- She has received over a dozen pieces of unsolicited mail at her home address in the name of the alias she only used with the shelter. These continue to expand as these companies share data with partner organizations.
- The email address that she provided on the adoption application now receives pet related spam daily. Advertisements for insurance, vaccinations, food, and safety gadgets flood that account, which she no longer checks.
- The telephone number she provided on the application was shared with a local veterinarian which has added it to a SMS text campaign. Every week, she receives unsolicited tips and reminders to arrange for various pet services (at a cost of course). She can terminate that VOIP number or simply turn off notifications for it.
- Her alias name and address appear in a premium database owned by Experian, which is searchable by anyone. More details can be found at www.experian.com/small-business/pet-owners.jsp. My client is not concerned, as the entry is not associated with her real name.
- 24PetWatch has updated their records to include her alias name and address within their database, which is accessible to thousands of people including practically every veterinary office in the country. If someone were to scan her pet's microchip, a social engineering pretext to a veterinary office could yield her name and address. Therefore, I advised that she update the record again. This time, she should use her same alias name but change the address to the shelter's location. If the dog is lost, the shelter will be notified. They have her alias name, address, and number on file to contact her. While unlikely, this could prevent an advanced attack if someone identified her alias name and address (and dog).

The next hurdles will be ongoing “maintenance”. Pets need continuous vaccines and licenses. When you obtain an animal from a shelter, the animal is almost always spayed or neutered, current on rabies and other vaccines, and “legal” in the county. Once you take possession, you are responsible for the continued medical care and licensing. Most counties in the United States have a legal requirement to maintain yearly rabies vaccinations. Part of this requirement is to register your pet with the county and pay a yearly fee when you provide proof of vaccination. Usually, your veterinarian will submit all of this for you as part of your visit for a rabies shot. You have a couple of options here, and I will list them in order of preference.

If you have already established yourself under an alias name with a local veterinarian, let them do the work. Show up for your yearly appointment, pay the fee for the visit and the vaccination, and pay the additional fee for them to file this with the county. They likely have rabies tags from the county on site and can issue your tag the same day. Part of this action will include them passing along your information to the county. To be fair, this will include your alias name and real address. If YOU sent this information to the county, it could be considered an illegal act. If THEY submit this data to the county, the act is a little less grey. Only you can decide if this is appropriate, but know that animal registration data is public record.

If you purchase and administer your own rabies and other vaccinations, you can submit any required paperwork to the county. The county is really only looking to enforce rabies vaccinations and is not likely on a data hunt about the owner of the pet. Do not lie on this form, as it is a government document. In my experience, placing the name of the animal in the line that is meant for your name suffices, as long as you also include the address, proof of vaccination, and the yearly fee. In that case, you have not provided false information, you simply excluded your name and instead provided that pet's name.

You may be shaking your head at this, but it matters if you have a need to stay truly private. In 2017, I had a client with a crazy stalker who knew everything about her. She relocated into an anonymous home, but obviously kept her pet. The crazy stalker contacted animal control in the county where he suspected she was staying, stated that he found a dog with a collar and tag with a very specific name, and hoped to return the animal. The county found only two pets on file with that unique name and provided the address for both of them. One was my client. It only takes a small mistake to ruin all of your hard work.

Another hurdle is boarding an animal. I am lucky that I have a trusted neighbor who takes my dog in when I travel. He has twelve acres of fenced land and Riley runs with his dogs the entire time I am gone. However, I have had to board him once when the neighbor was unavailable. Gone are the days of dropping off the dog, leaving some cash, and picking it up later without many questions. Practically every professional boarding company will want proof of vaccines, veterinary records, and your personal information.

I chose a local outfit which had great reviews and visited it with Riley. Since it was my first time there, I had to complete an application and sign consent allowing the sharing of any data to third-party entities. It is almost impossible to escape this throughout our daily grind. I provided my alias name and an alias hotel address. I keep redacted copies of Riley's records for events such as this, and they accepted that as proof of rabies, Bordetella, and other vaccines. I purposely redact the name and address of the vet, as that should never be shared. That did not fly in this scenario. They demanded to know the name of the vet and stated that they would contact the office to obtain their own copies of Riley's records.

The problem here was that my vet does not know the name Riley and possesses yet another alias address. Since the vet office did not obtain my record from the shelter, they do not have my real home address. This can become difficult to manage quickly. Thinking as fast as I could, I provided my veterinary office information and told her that Riley is likely listed under Kosmo. I blamed this inaccuracy on me getting him from a shelter and they sent over the paperwork to the vet from when he entered the shelter. Not my perfect execution, but not too damaging either. She retrieved the records from the vet, including the alias address I had given them, and Riley entered a temporary home while I visited a client.

The outcome of this experience included several undesired communications. I received spam email messages from the boarding provider to my alias email provided to the veterinarian, which they obtained from the records sent over. I received unwanted SMS text messages on the burner number provided to them reminding me that they had new obedience classes. I probably received physical mail in my alias name at the random hotel addresses provided to the vet and the boarding service. I anticipated that my contact information would eventually be leaked to other related companies. When it did, there was not much concern, as they did not have my name and true address. In 2020, I received an email from a previously unknown vet in the same city as the boarder. The email confirmed Riley was due for updated vaccinations, as determined by the records sold to this vet by the boarder, which were copied from my original vet. Animals have no privacy either.

For the record, I no longer use boarders, as I find having close relationships with friendly neighbors with dogs is much more beneficial. They don't ask questions, demand ID, or want to see vet records. My dog is much happier when I return, and I have found that a surprise 50-pound bag of the neighbor's desired dog food left on his porch enables future stays.

In 2020, I encountered a new privacy issue in regard to pet care. My dog needed an expensive long-term prescription which is also available for humans. My vet encouraged me to have the prescription filled at Walmart, as it would be much cheaper. After learning the substantial price difference from an expensive pet brand medication versus a generic option from Walmart, I was convinced to take the prescription and have it filled on my own. Walmart agreed to fill the prescription within the local store's pharmacy, but demanded to photocopy my government-issued photo identification. I walked out empty-handed. However, Walmart, Chewy, and other providers offer online prescription orders with delivery directly to you. Identification is not required for online prescriptions, aliases can be used, and private forms of payment are accepted. However, there are other issues. The following happened to my client mentioned previously in this chapter.

Her vet directed her to a third-party supplier called VetSource for her monthly medications required for her pet. The vet even provided a discount code in order to save money on the first order. She went to the site, added her medications to the cart, and proceeded to check out. The service already knew the identity of her vet since she used a referral link from the vet's website, and VetSource informed her that they would need to verify her prescription with the vet before the order could be placed. She had used an alias name and true address with the Vet, but intended to use her real name and credit card for medications which would be shipped to a UPS box. She felt stuck. Any name and address on this order would be shared with her vet, and the order would probably be declined. In this scenario, she decided to use her real address and alias name for the order. The vet already knew this address since the adoption records displayed it. The vet confirmed the order and quarterly packages arrive automatically, being charged to a Privacy.com account.

I present this situation as the reason we must always have a solid plan before executing any privacy strategies. During the first visit to the vet, know the name and address which you will be using. This will be on file forever. If you need to have home deliveries of medication or the ability of home visits, plan for that. For most clients, I recommend providing an alias name, actual home address, and a masked form of payment. This can be a service such as Privacy.com or a prepaid credit card. Personally, I keep a prepaid Visa for use only with my vet. There are many benefits of your pet publicly belonging to your true home address. If he or she is lost, return can be made quickly. This also serves as some decent disinformation, as explained in a later chapter.

In most situations where you are obtaining any type of in-person service for your dog, cash payment should be acceptable. I never use a personal credit card, even a secondary alias card, for anything associated with my dog. You may still be wondering why my dog has alias names. It was unintentional at first. When I adopted my dog, he had a temporary name of Lightning. This was given to him when he arrived at the shelter because no one knew his real name and he was a bit wild. When I adopted him, I had no reason to advise the shelter that I would not be using that name, especially since he did not respond in any way to it, and that I had started calling him Riley. To this day, the shelter believes his name is Lightning.

Out of paranoia, I did not choose a veterinarian from the suggested list provided at the adoption. I sought my own option and took "Riley/Lightning" in for the next round of vaccinations and a checkup. On the new patient application, I provided the name as Kosmo. I don't know why. It just happened. I guess it is just habit. I was not using my real name, why expose his? I projected feelings of approval for this behavior from Riley, and my vet calls him Kosmo to this day. This was all fine, until it wasn't.

While at a local dog park, I encountered an employee from the shelter where I obtained Riley. We talked briefly while our dogs played, and then my vet showed up. He asked how Kosmo was doing, which seemed to surprise the shelter employee who had been calling him Lightning for the past 30 minutes without any correction from me. In an awkward tone, I called out "Let's go Riley!", and we left, likely adding more confusion. Maybe an alias for a dog is overkill.

This brings up another consideration. What information do you place on a pet tag? In previous years, I would say it really does not matter. Today, I have a firm opinion on this. I believe a pet tag should only have one piece of information on it. It should only include a reliable telephone number which can reach you at all times. I use a MySudo number for this, but you may have other VOIP options. Most tags have a pet name, owner name, address, phone number, and email. The following explains my reasons to exclude most of these details.

- Pet name: Why is this necessary? Will that determine whether a person that found your animal will call you? I do not believe so. This also prevents you from ever giving some stranger a wrong name for your pet.
- Owner name: This one is obvious. Any name I provide would be fake anyway. Anyone that finds my pet will not know me. Again, this locks you into a specific alias name when you are out with your animal.
- Address: If you are comfortable with exposing your home address without a name, this is not a huge issue. My reservation is during the creation of the tag. You have likely seen machines at pet stores which allow you to create your own custom tag. These are very affordable and provide an immediate result. They also share those details with affiliate companies. Think about the potential. If you owned thousands of machines in big pet stores that made pet tags, and you obtained the names, addresses, and phone numbers of the owners, you would have some valuable data. Pet supply and insurance companies devour this data and bombard users with unsolicited offers. I do not want to share my home address, regardless of alias name.
- Email: Aside from the previous reason, email addresses are more prone to spam. I also suspect that anyone who found my pet would rather call and may not bother sending an email. Additionally, burner email addresses could expire when not used and you may not receive the message. You are also trusting the ability to avoid typos from the finder.

For these reasons, my dog's tag has only a telephone number. I find that to be sufficient. Do you need to provide an alias name to associate with your pet(s)? Only you can answer that. I hope that this chapter has provided some insight from my experiences, and exposes the data leakage that happens when you possess an animal. My final thought to close this chapter is that numerous entities want a piece of the action in regard to your pet. Pay the legally required licensing (county/city fees), provide the legally required care (rabies and other immunizations), and stay out of scope from anyone tasked with holding people accountable. Play by the rules, but never provide more personal details than necessary. Surprisingly, minimal information disclosure is required, but we tend to give in to marketing tricks.

CHAPTER FOURTEEN

BEYOND EXTREME

You may believe that the privacy strategies presented in this book are a bit too complex for your needs. For many of my clients, the previous pages represent only the basics, and there is a desire for the next level of privacy. Some clients need extreme protection through name changes, dual citizenships, or various uncommon legal documents. Most people reading this may need none of that. However, in the rare situation where you are targeted by a powerful adversary, these are tools to possess in your arsenal of privacy strategies. Before proceeding, let's have a quick reality check and consider your progress.

Until now, I have focused on the most popular services which my clients request from me. Moving to an invisible home, driving an anonymous car, and communicating from sanitized electronics are very normal in my business. These are the things which I encourage you to implement. Traveling full time, changing your name, moving to another country, giving birth to expedite citizenship, and planning the details after your death are rare, but I have assisted in these situations. This chapter represents the extreme of the extreme. Please do not execute any of these strategies without seriously considering all potential consequences. Of everything discussed in this book, the methods explained in this chapter backfire the most. For many, this content may just be an entertainment break before jumping back into common strategies. For others, it may save their lives.

Readers of the previous edition of this book offered criticism of the placement of this chapter. Many believed it should have been presented at the very end of the book. This is valid feedback, but I chose to leave it in the current chapter lineup. This chapter navigates us toward the end of our PROACTIVE journey toward extreme privacy. In the next chapter, I transition to methods for damage control, which are more defined as REACTIVE.

You may be tempted to skip this chapter and move on to more applicable topics. The content within this chapter is not necessary in order to implement later tutorials. However, I hope that you will indulge me by considering the topics presented within the next several pages. If you ever find yourself stuck within an exceptionally rare threat, you may need to rely on these extreme methods.

The RV Life

In previous chapters, I discussed ways in which nomad residency could be obtained in order to provide a true ghost address for government documentation. This instruction took advantage of rules and policies designed for full-time travelers without the requirement of living out of an automobile while exploring the world. In 2021, I assisted more clients with becoming truly nomadic than in the past decade combined. This section explains the process of committing to a life of constant movement.

Most people who are nomads in South Dakota rarely visit the state. They have a recreational vehicle (RV) and stay within warm boundaries at all times. They visit their favorite RV campgrounds in Florida during winter and northern cities in summer. They have eliminated most of their belongings and crave a life of freedom while having the ability to pick up and go at any time desired. I respect that lifestyle, but it is not quite what I present to my clients. During this section, I will assume you have an urgent need to disappear, and that you are not ready to commit to the purchase of an anonymous home. You may not know where you want to go, and you may have concerns about making mistakes while creating trusts, LLCs, and your personal privacy strategy. Becoming a true nomad eliminates some of these stresses while providing a quick exit. The following actions were taken by a client in 2021.

“Jeni” left an abusive relationship with a tech-savvy man and needed to disappear. He had made numerous threats to end her life after she left him. There was no time for a home purchase and she had no friends or family outside the small town which she lived. She had not traveled much and had no ideas about where she wanted to live. My immediate recommendation was to obtain an RV and take some time to collect her thoughts.

The first decision is whether to rent or purchase. For most clients, I always recommend renting before purchase. Many people learn quickly that living in any type of automobile is not for them. The tiny kitchens, tight sleeping areas, and overall lack of any privacy can become too much to take long-term. Other clients adapt quickly and commit to a life of mobile living. Another benefit of renting is the absence of any vehicle registration requirements. You can hit the road and be fairly untraceable with minimal effort. Jeni chose this route.

She rented a small class B Airstream which provided plenty of room for her. It had the appearance of a large extended van. She confirmed that her current vehicle insurance covered her and the rented vehicle. She established a South Dakota PMB and forwarded all mail permanently to it. She changed her address on all important accounts. She drove the RV to South Dakota and applied the previous lessons to obtain a new driver’s license. She stayed at a local campground the night before, and provided a receipt to the DMV to meet the nomad qualification. She was now a legal nomad with a new DL and ghost address. She technically lived in her RV and began identifying campsites where she could spend some time.

Jeni obtained a new mobile device, prepaid cellular plan, VOIP phone calling options, secure communications, and masked debit card service. She never provided her real name; paid most of her camping fees in cash; and collected her mail at campgrounds right before she left for another area. She was invisible. She later met a new partner and they traveled the country together. This fairy tale is not as simple as I present it. Let's take a look at the problems you might face in this scenario.

Downsizing: If you plan to go mobile, you will need to eliminate everything unessential to your life. Space is extremely limited and valuable while you travel. I recommend either storing your belongings before leaving or eliminating them altogether. I have been through this process, which can be difficult. I found that photographing memorabilia, awards, and other sentimental items eases the pain of getting rid of them. Digital scans of all important documents, photos, and paperwork eases the transition to mobile life. Make sure you have strong backups of everything.

Insurance: Some providers do not insure rental vehicles, and those that do may not cover RV's. If your provider will not offer coverage, contact a local insurer in the county of your new PMB. They are very aware of the requirements.

ID Requirements: Many campgrounds and RV lots require identification upon entry. Most do not scan them, but I have found some which do. I do not object to showing ID, but I demand that a scan is not collected. I have found that a polite request to avoid any scanning or collection works most of the time, especially with independent campgrounds. I try to avoid any national chains.

Purchase: If you want to buy your own RV, there are more complications. I recommend establishing your PMB first; then purchasing the RV in the name of a trust, and then registering the vehicle within the PMB state.

Registration: If you purchased your own RV, the state will allow registration in the name of a trust with a mandate to know the true information of the trustee (likely you). I find this acceptable for two reasons. First, your name will not be publicly attached to the registration plate. Even law enforcement will not receive your name with a standard license plate check. Only the DMV can disclose your name and PMB after an official request. Next, if your name is associated with a place which you never visit again, there is minimal threat.

Food: If you enjoy cooking large meals in a full kitchen, you will be disappointed. Outside of a hotplate and miniature refrigerator, you don't have much of a kitchen. However, always keep a few comfort foods available which remind you of home. I have found this uplifting during extended travel.

Internet: For light browsing, you may find your mobile device's data plan sufficient for primary internet access. You can enable a VPN on both the device and your laptop, then allow your device to share internet wirelessly. For heavier users, you may want to purchase a dedicated portable internet device.

Expense: A nice RV can be very heavy in weight. This results in low mileage per gallon of gasoline and high fuel costs. I have been naive to this and surprised at the frequency of gas stops and high costs. If you need to be untraceable, make sure to carry plenty of cash without relying on ATM withdrawals. If you need water and electric hookups, expect to pay a premium for these services. Do your research before you commit and be overly prepared financially. When you get desperate, most Walmart stores allow overnight parking for free.

Social: Living as a nomad, especially if you are alone, can be emotionally burdensome. However, it can also be a great opportunity to make new friends. When I have tried to strike up a conversation while staying at an extended-stay hotel, I was perceived as a creep with bad motives. When I repeated that same conversation at an RV campground, I was welcomed into the conversation; offered food and drink; and encouraged to return the next evening. I believe you will find an easy time meeting other people if desired. You can also make up practically any alias and former life without worry of criticism or judgement.

Children: One surprising advantage of living in an RV is the ability to easily register children for school. Schools want to know your true physical home address which complicates privacy. If you are staying (even temporarily) at a local campground within the boundaries for a specific school system, you should qualify for registration. This will always vary, but most public schools do not fight it.

Stability: Many clients feel an uncomfortable sense of instability. The few belongings they have are with them at all times and there is no physical home waiting for them after the adventure. I see this kick in about three weeks on the road and disappear after two months. Everyone will be unique.

Freedom: I want to end this on a positive note. I have talked with numerous clients while they were living a truly nomadic lifestyle. The common sentiment was an appreciation for the overall freedom, privacy, and security they felt. The ability to move around fairly anonymously is comforting to those who are running from a legitimate threat. Traveling by vehicle while purchasing fuel with cash eliminates most common travel tracking possibilities. The lack of airfare history, hotel stays, and rental vehicle contracts prevents the common methods which are used by abusers to locate victims.

Name Change

For the record, I almost never recommend a name change (outside of a traditional change associated with marriage or adoption). Changing your name does not carry the power it once had in previous decades. Today, your new name is likely to appear as an alias on your consumer profiles within data mining products. This is because your new name is still associated with your current SSN. Additionally, some states and counties require your name change to be publicly posted, such as within a local newspaper. Digitization and permanent archiving of these details will not keep them hidden long. For clients who are insistent on a name change, I follow a specific recipe.

First, I run them through the nomad residency process through South Dakota as previously explained. I obtain a new license in their official name, and then wait. Six months after residency, you are allowed to petition for a name change. The required forms can be found on the South Dakota website at <https://ujs.sd.gov/Forms/namechange.aspx>. The process begins with a petition for change of name, followed by a hearing, and finally an order if the change was approved by a judge. All of this will require physical presence within the state and multiple court visits over the period of a couple of months.

This process is very similar in other states. The difference is the privacy. Many states, such as California and New York, make court records public on the internet. This is becoming the default action as most states digitize all historic records and place them online. Some more populated states allow third-party companies to devour this data electronically via application programming interfaces (APIs). In other words, many states allow companies to automatically suck up all court documents in order to populate their own data mining systems. South Dakota is much more reserved. While a name change is public record, unless a judge can be convinced it should be sealed, South Dakota does not go out of their way to notify the world. In my experience, it is not difficult to convince the court that a name change should be sealed (private) in scenarios involving physical attacks toward the victim. This will not make you invisible as your true privacy threat is your SSN and DOB combination.

If you are going to change your name for privacy reasons, you really need a new SSN in order to stop the association. Even then, it will be easy for companies to determine you are the same person. Changing your SSN requires a visit to a Social Security office. You will be required to show ample identity documentation and your current Social Security card. This is not an immediate process, and your old number will remain present within many systems. Your case will be evaluated, and a new number may be denied. If issued a new number, expect problems with any attempts to establish new credit. If you do require a new credit card or loan, the new SSN and the old will be permanently connected, which removes any privacy strategy here.

Overall, I do not recommend name changes and/or a new SSN. In order to possess any privacy, you can never obtain any new credit or use your new name and SSN on any official documentation. This will be difficult. If you slip, you associate the old information with the new. I believe that you can achieve the same level of privacy by executing the previous methods displayed throughout the book. With permission, I provide the following undesired result after a name change was conducted for a client.

In 2019, “Janis Doe” had become a South Dakota nomad. Her PMB was the only valid address on any public or private record. Her condo was in the name of a trust and her vehicle titled to an LLC. Her utility companies had no clue of the identity of the occupants in her home. In my opinion, she was invisible. She contacted me with a desire to change her name as a final strategy to eliminate her past. After encouraging her to avoid a name change, she insisted on moving forward and I began the process.

We submitted the paperwork with the state and she made her appearances in front of a judge. Due to her experiences with physical abuse, the court agreed to seal the record. Within a few weeks, she was now “Janis Smith”. She obtained a new driver’s license in this name, applied for a new passport, and she now had a new identity. Eventually, the Social Security Administration confirmed they recognized the change but delayed issue of a new SSN. That is when the real problems began.

When she notified her bank of the name change, they insisted on sending a physical form which would need a “wet” signature and notary. She provided her PMB address which was flagged as a CMRA mail drop. The bank refused to send anything to that location. Since they wanted to verify a physical address, stopping by a local branch would not help. Until she provided her true physical address the bank refused to update her information. After a few visits to a local branch, a manager finally agreed to file the paperwork on her behalf. This was the beginning of the paper trail which would ruin her efforts. Her insurance policies, credit cards, and retirement accounts were all updated, and each of them added to the trail. As I write this in 2020, a search of this “Janis Smith” within every premium data mining company to which I have access reveals her to have an “also known as (AKA)” entry for Janis Doe. A search of her old SSN immediately connects to a record of the new SSN. The two identities are very connected and she has no real privacy protection from the name change.

Today, I believe there is no reason to change your name or SSN, aside from emotional scars from family issues. These changes will not erase your financial, residential, and family past, and will always leave a trail which combines the two identities. The name changes of fifty years ago were effective. Today, they are just cosmetic.

Marriage Considerations

The physical location of your marriage can have a huge impact on your privacy. Consider two states which approach public access to this type of information very differently. New York provides public access to all records via a dedicated division titled the Vital Records Office at the New York State Department of Health. Their website proudly announces that every marriage (and divorce) record from 1880 to present is available to anyone online. A simple search form is provided for immediate access. In contrast, Colorado's state law (C.R.S. 25-2-117) declares vital records such as birth, death, adoption, marriage, and divorce as confidential. As a result, Colorado vital records are not public records; therefore, they are not searchable online. Vital records can only be released to those who are eligible, such as the bride, groom, or an immediate family member. These are only two examples. You should research the laws and policies of any state where you are considering marriage.

If you had your mind set on a California wedding, you have a surprisingly private option. California is the only state which offers both a regular public marriage license and a confidential marriage license. A confidential marriage license is legally binding but not part of any public record. Section 501 of California's Family Code allows the county clerk to issue this option. Section 511 states that these licenses are not open to public inspection except by a court order. However, public marriage licenses allow anyone to look at the personal information that appears on the licenses at the county clerk's office. This includes the couple's names, dates and places of birth, parents' names, and any previous marriages.

I have been asked on several occasions whether a confidential California license is better than a public license from within a state which does not allow online search of marriage records. In most scenarios, I believe the California confidential option is better. If a state which is fairly private now, such as Colorado, later changes to a public record model, your details could become publicly shared with third parties. I believe this is less likely with an intentionally confidential license from California. Many states offer an option to have the court seal the record, but this brings unwanted attention to you, and you will be forced to convince a judge to protect your privacy. I prefer more streamlined options.

Overall, I recommend that privacy-seeking clients apply for a marriage license, and execute the ceremony, outside of their home state. This provides a small layer of privacy. Many automated people search databases will associate marriage records from within a specific county to people with those names from that county. Marriage records from distant counties may not be automatically added to a person's profile. However, if the public marriage record includes dates of birth and parental details, it will likely be associated with the individuals anyway. This is why I push clients to become married in states which respect the privacy of the marriage, and are at least one state away from their home. Always contact the county of potential marriage to identify whether the details are publicly shared.

The next consideration is name changes due to marriage. In the United States, it has been customary for the bride to take the surname of the groom. I believe this is very traditional thinking which has not kept up with our current society. Today, it is very common for each spouse, regardless of gender, to keep their own surname. In most scenarios, I believe this is best. It is not only convenient to avoid countless name change forms, but it also provides two last names which the couple can use when necessary. Consider the following scenarios.

- A spouse with a very unique name is heavily targeted with online threats. The spouse with a common last name can hide more easily within online records if the name should become public after utility or delivery details become public.
- The same targeted spouse feels uncomfortable associating his last name with the couple's new home, but the HOA demands a confirmed resident be listed within the neighborhood records. The spouse with the more common name, who is not targeted, could be included in the documentation, with less threat.
- In contrast, a spouse who is being heavily targeted could decide to take the last name of the spouse with a more common name in order to provide a slight layer of privacy.

In each of these scenarios, the protection is minor, and does not replace the privacy strategies explained throughout the book. If executed properly, your name(s) will never be associated with your home, and none of this may matter. However, backup plans are always nice. Next, consider the privacy invasions of online wedding registries. These require you to publicly disclose the names, location, and general details of your upcoming wedding and attendees. This information is later sold to other companies in the wedding industry. You are also required to disclose a physical address to which your gifts can be shipped. I encourage you to eliminate this marketing scam from your wedding. Your family and attendees will likely revert to the old-fashioned gift-giving methods from a pre-internet era.

Reality Check: Modifying the plans of your marriage may present a new layer of privacy desired by you. However, consider the feelings of your spouse. Refusing to take a married name (or refusing to give it) could create serious strain on a new marriage. Hiding the details from public view may generate a suspicion of embarrassment in the relationship. Never execute these strategies without seriously discussing it with your partner. If there is hesitancy or a sense of confusion and discomfort, take a step back and identify the issues. For me as well as my clients, family relationships are more important than the desire to disappear. If your partner is on board with all this extra effort, you may have found your match. Approach cautiously and do not blame me when you are left at the altar because you did not consider the wishes of your mate.

Birth Considerations

Many childrens' birth certificates are public record. While we do not see them copied into people search websites, the data itself can be usually seen or verified by anyone willing to visit the county seat and claim to have a need for a copy of the record. Worse, services such as VitalChek (a LexisNexis company), allow practically anyone to order another person's birth certificate online by confirming a relationship and need. While writing this section, I provided publicly available information about myself to VitalChek. I stated I was a relative and the service authorized me to obtain my own birth certificate as a genealogy researcher. The cost was \$20 and anyone could have replicated this by knowing only my name, date of birth, and mother's maiden name. All of these details can be found online about most of us.

Similar to marriage records, states such as California make birth certificates easily available to data mining companies while states such as Colorado consider them confidential. Let's consider the data required to complete a birth certificate which could become public. Most states require the following information, which is usually submitted by a medical attendant.

Child's Name	Location of Birth	Parents' Places of Birth
Child's Gender	Parents' Names	Parents' Signatures
Child's Date of Birth	Parents' Dates of Birth	

This information may not seem too sensitive to most. A home address is usually not present unless the birth occurred at home. However, I respect that some clients do not want these details released publicly. Some may be keeping a relationship secret, while others do not want any clues about the county in which they reside available to a stalker. Regardless of your situation, extreme privacy enthusiasts may desire to keep a birth certificate private. Some states have specific laws which declare birth certificates confidential and only available to immediate family. However, I find this to be a small hurdle to bypass. While illegal to access someone else's birth certificate without family authority, people do it anyway. I encourage clients in extreme situations to assume that the birth certificate for their child will become public record. Therefore, they should consider the key data which will populate the document.

Location: If I know the county in which you live, I know where to search for a birth certificate. If you choose to give birth in another county, this makes my search more difficult.

Name: If I know the name of your child, possibly if it were posted to social media, I would have enough information to conduct a search. Preventing details of your birth from appearing on the internet eliminates the easiest way to obtain a copy of the birth certificate.

While we are discussing names, we should address privacy implications of naming a child. The less unique his or her name is, the greater your child's privacy will be in the future. A person

named John Smith may be much more difficult to track than one named Michael Bazzell. Finding the right John Smith would require substantial time to sort through thousands of records. If you have a common last name, you are already at a huge advantage over those who have unique surnames. There are still steps you can take to make your child's name less distinguishable.

While I respect that passing a family name to a child is a traditional and important piece of family history, there are extreme situations when this may be avoided. I have witnessed the following.

- Some privacy enthusiasts will choose the desired name with which they wish to address their child, but make it the middle name. If they desire to call their child Michael Bazzell, they might make the official name John Michael Bazzell. This results in most people search sites identifying the child as John Bazzell. People who know him as Michael Bazzell might not identify this association.
- In one scenario, a couple did not possess the same last name. They were married, but the wife never changed her name to match the husband. They decided to "mash-up" their last names and provide their son a unique last name. Assume the father's last name was Bazzell and the mother's name was Singleton, the child's last name was similar to Baton. Obviously, this is a fictional example in order to protect the privacy of the real parents and child.
- Some choose to issue numerous middle names to a child. John Michael William Bazzell could legally use John, Michael, Mike, William, Bill, Billy, or Will as a legal name at any time. This provides numerous legal aliases ready for the future.

The next consideration is the Newborn Genetic Screening test, which is required in all 50 states. Nearly every baby born in the United States gets a heel prick shortly after birth. Their blood fills six spots on a special paper card. It is used to test for dozens of congenital disorders which, if treated early enough, could prevent severe disabilities and even death. Some states destroy the blood spots after a year. However, many states store them for at least 21 years. California is one of a few states which stores the blood spots for research indefinitely. These results are often given to researchers, queried by other government agencies, and sold to private corporations. You pay the fees for this mandated test.

Most hospitals provide information about this data collection and your rights according to the specific state where the child was born. Most states require submission of a card which either allows consent to share the data collected or explicit refusal to participate in the program. Some parents may choose to omit their child's blood sample from any state or national databases. Many people report that the samples are collected and shared if no action is taken after birth. I encourage you to identify this consent form and consider your options.

It is desired, notify the hospital that you do not want a birth announcement in the local newspaper. A surprising number of hospitals provide this data without parental consent. In 2021, I consulted with a client concerned about child birth privacy and health safety during the COVID-19 pandemic. After many conversations, they settled on a birth center with a midwife. A birth center is a health care facility for childbirth where care is provided in the midwifery and wellness model. A birth center is typically freestanding and not a hospital. Birth centers are well known for respecting a woman's right to make informed choices about her health care and her baby's health care based on her values and beliefs. This can create an environment for a much more private experience compared to a traditional hospital. My clients witnessed the following benefits.

- Birth centers typically have fewer deliveries at any given time with proper staff for each patient. This may prevent random and unfamiliar staff entering and exiting at all times.
- Private rooms are much more common at birth centers than maternity wards.
- Hospitals typically demand government identification from visitors, which are often scanned into insecure systems. Birth centers have more leniency on these requirements.
- The midwife typically completes the baby's application for recording of birth and can offer to send the state documentation via USPS instead of digital transmission online. Many states share application data submitted electronically with third parties such as VitalChek, the service previously mentioned which is owned by LexisNexis. These companies then charge the public fees to access documents, such as a birth certificate, of your child. Per the VitalChek privacy policy, they reserve the right to share your personal information with their affiliates, technology providers, customer service representatives, service providers, suppliers, editors, payment processors, and email service providers.
- Genetic screening tests are optional and not required by the birth center.
- Birth centers typically provide more education on your privacy-related options as parents.
- Many birth centers allow payment to be made in cash for the entire visit. My client's final bill was \$5,200.

Choosing the method of child delivery is a very personal decision and should never be made solely on the recommendations of a privacy nerd like myself. I present this page as an option to initiate a conversation with your family about privacy considerations during childbirth.

Death Considerations

Let's get gloomy. We are all going to die. For some, our privacy shenanigans may not matter after we are gone. For others, including myself, our death may be the opportunity to apply one final privacy strategy. Most of my clients are not concerned with keeping death details private, but we should all consider our families' needs once we leave. Anything we can do now to ease the decisions surrounding our passing will be welcomed by those faced with the responsibility. Let's start with some additional documentation which may be helpful.

Final Arrangements Document

Most states do not have any specific laws about the validity of a Final Arrangements Document, also known as an End of Life plan, Final Wishes Planner, or combination of any of these terms. Typically, this is a document outlining your final desires related to your funeral, public death announcements, disposition of your body, and service details. This may not be considered a legal document, but it can be extremely helpful to those planning your funeral and death announcements. First, let's consider why we may desire such a document.

People search websites scrape online obituaries for deceased family member's details. They then populate the newly discovered data into their invasive systems. Consider the following demonstration. You are a very private person and your mother passes. A traditional obituary will publicly display your full name, spouse's name, actual city of residence, children's names, and relationships to all siblings, nieces, nephews, etc. People search websites devour this data and append your profile. Within weeks, you are listed within dozens of websites which accurately identify your location and family members. If this bothers you, a Final Arrangements Document can protect your relatives when you pass.

Please note this document is not publicly filed with any government entity. A Notary signature is not required, but witness signatures are vital. I also encourage you to explain this document and your wishes to immediate family. You do not want someone challenging the validity of this document. I have witnessed funerals which were conducted in a completely opposite manner as the deceased intended due to arguments among the children.

The following page presents a sample document with fictional information. This can be modified in any way desired to meet your own demands. I present this only as a guide. For some, this may remain a single-page directive. Others may incorporate elaborate details. Most readers will rely on this document in order to prevent personal details from being shared publicly through death announcements and obituaries. It also specifically outlines a desire to prevent personal information from being shared through social networks.

Final Arrangements Document for John Wilson

I, John Wilson, currently of Los Angeles, CA, being of sound mind, willfully and voluntarily declare that these are my final wishes as to the disposition of my body after my death and any services or memorialization to be held in my name. This document is not intended to be interpreted as my Last Will and Testament.

APPOINTEE: I request that Jane Wilson be in charge of executing my last wishes.

DEATH ANNOUNCEMENT: I wish to have a death notice submitted only to the LA Times. My death notice should include my date of birth as January 1, 1980 and my birthplace as Los Angeles. It should not include the names or locations of any family members as respect toward their privacy. I do not wish any details of my funeral or other services be included in my death notice. I request my death notice to exclude any residential, hobby, or employment history. I request that any death announcements be omitted from any social networks or online forums, including, but not limited to, Facebook, Twitter, Instagram, and Snapchat.

ORGAN DONATION: I wish to donate my organs upon death and am a registered organ donor in the state of California.

DISPOSITION OF BODY: Upon my death, I wish my body to be cremated. I wish for my ashes to be scattered as desired by Jane Wilson.

SERVICES: Upon my death, I wish to have a private memorial service to commemorate my life. I would like it to be held at the Elks Lodge, located in Torrance, California, if possible.

FINANCING & EXECUTION: I have set aside funds to cover my expenses which are located in my safe. I request that Jane Wilson follow the spirit of these wishes as well as she can and within the limits of any applicable law.

John Wilson

Date

Witness Name

Witness Name

Witness Signature

Witness Signature

Date

Date

Living Will (Instructions for Health Care)

A Living Will does not outline your desires for distribution of assets after you die. Instead, it is a legal document which explains medical directives while you are alive. This document likely exceeds the scope of this book, and has very little relationship to privacy. However, it fits well within this section and can provide value to those already making end of life decisions. First, consider a few reasons why you may need a Living Will.

It Protects You When You Cannot Communicate: The biggest advantage of having a Living Will is that it protects you in a future situation during which you no longer can communicate your wishes. Otherwise, medical professionals in charge of treating you have the authority to choose your treatment on your behalf once you are in a state in which you cannot communicate what you want to be done.

It Prevents Arguments Between Family Members: Medical care decisions can cause a lot of trouble among family members. If they disagree on what should be done, it can cause relationship-ending arguments. With a Living Will, it will be your choice and no one else's. This should help eliminate any argument or debate as to what should happen to you.

It Gives You Control Over Medical Treatments: A Living Will provides you complete authority over which medical treatments and procedures take place in a situation where you are unable to communicate. In this specific situation, a Living Will legally demands doctors to fulfill your wishes and removes the decision from them.

It Reduces Potentially Unwanted Medical Bills for Your Family: In the situation that you get into a coma or vegetative state, a Living Will determines healthcare action. Some people would rather die than live an additional 20 years on life-support. This is usually due to the enormous medical bills for which their family will have to pay while you are miserable. If you do not want to see something like this happen, you need a Living Will that specifies exactly what you would like to happen in a given situation.

It Provides Peace of Mind: Finally, Living Wills are designed to give you the control to prevent more bad things from happening in already tragic situations. You may want to know that your family, as well as yourself, will be taken care of properly in such a situation.

I encourage you to be proactive while considering your desires for end of life decisions. Don't surrender control over what happens to you under bad circumstances. The following document contains the basic language of a Living Will. You can also find numerous templates online which contain more detailed information. Choose a document most appropriate for your desires.

INSTRUCTIONS FOR HEALTH CARE

END-OF-LIFE DECISIONS: I direct that my health care providers and others involved in my care provide, withhold, or withdraw treatment in accordance with the following:

Choice Not To Prolong Life: I do not want my life to be prolonged if (i) I have an incurable and irreversible condition that will result in my death in a relatively short time, (ii) I become unconscious and, to a reasonable degree medical certainty, I will not regain consciousness or (iii) the likely risks and burdens of treatment could outweigh the expected benefits, OR

Choice To Prolong Life: I want my life to be prolonged as long as possible within the limits of generally accepted health-care standards.

ARTIFICIAL NUTRITION AND HYDRATION: If I have selected the above choice NOT to prolong life under specified conditions, I also specify that I do or do not want artificial nutrition and hydration provided to me.

RELIEF FROM PAIN: I direct that treatment for easing pain or discomfort be provided at all times, even if it hastens my death.

EFFECT OF COPY: A copy of this form has the same effect as the original.

REVOCATION: I understand that I may revoke this OPTIONAL ADVANCE HEALTH CARE DIRECTIVE at any time, and that if I revoke it, I should promptly notify my supervising health-care provider and any health-care institution where I am receiving care and any others to whom I have given copies of this document. I understand that I may revoke the designation of an agent only by a signed writing or by personally informing the supervising health-care provider.

John Wilson

Date

WITNESSES:

Witness Name

Witness Name

Witness Signature

Witness Signature

Date

Date

Traditional Will

In previous chapters, I explained the privacy strategies when using a trust to hold assets. During the discussion about living trusts, I explained that they have more power than a traditional Will because a trust does not go through probate. However, I do believe that everyone should also possess a traditional Will. It can be a “catch-all” document to address any concerns with assets which were not included in any trust.

A traditional Will does not necessarily offer much privacy benefit. My goal within this section is to identify additional unconventional details which can be beneficial to a privacy enthusiast. While a Will should not become public information, you should be cautious of its contents. During the probate process, practically anyone can claim they should be able to see the Will in order to potentially protest the validity. This is not common, especially with close families, but something we should consider. I have never seen the details of a Will become part of a people search site, so we can (and should) include family member details.

The following two pages include common language used within a Will. You should consult an attorney before executing your own Will, especially if you possess substantial assets. In order to keep within the scope of this book, I will only emphasize the items included in section (7) titled Special Requests. This area allows you to enter any details which would normally be absent from a Will. Since this is a legal document, as defined by the Will laws of your state, it may hold more power than any previous documents we have created. Specifically, consider my reason for including the following items.

- (7.1) I direct that my Final Arrangements Document be executed upon my death.
- (7.2) I direct that details of this document are not to be shared publicly or online.

The first item (7.1) provides some legal coverage for the Final Arrangements Document we previously created. This is likely not necessary, but may give cooperating family members leverage over those who wish to defy your desires within that document. The second option (7.2) is fairly vague and may have no consequences if ignored. However, having your desires to keep this information private, while visible to the entire listing of beneficiaries, may ensure that your requests are executed properly.

Some may question the need for a separate Final Arrangements Document, which was explained previously as a way to handle your funeral and public details, instead of simply including those details within a traditional Will. There are two reasons a single document is inappropriate. First, a Will is often viewed and executed weeks or months after death. The details are often ignored until after the funeral, which eliminates any chance of the end of life desires being granted. Second, a Will must go through probate and can be contested. I believe these documents should be separate.

LAST WILL AND TESTAMENT of JOHN WILSON

(1) Declaration: I hereby declare that this is my last Will and testament and that I hereby revoke, cancel and annul all Wills previously made by me. I declare that I am of legal age to make this Will and of sound mind and that this last Will and testament expresses my wishes without undue influence or duress.

(2) Family Details: I am married to JANE WILSON, hereinafter referred to as my spouse.

(3) Appointment of Executors:

(3.1) I hereby nominate, constitute and appoint JANE WILSON (SPOUSE) as Executor or if this Executor is unable or unwilling to serve then I appoint MICHAEL WILSON (SON) as alternate Executor.

(3.2) I hereby give and grant the Executor all powers and authority as are required or allowed in law, and especially that of assumption.

(3.3) Pending the distribution of my estate, my Executors shall have authority to carry on any business, venture or partnership in which I may have any interest at the time of my death. My Executors shall have full and absolute power in his/her discretion to insure, repair, improve or to sell all or any assets of my estate. My Executors shall have authority to engage the services of attorneys, accountants and other advisors as he/she may deem necessary to assist with the execution of this last Will and testament and to pay reasonable compensation for their services from my estate.

(4) Bequests: I leave my entire estate to my spouse, JANE WILSON.

(5) Remaining Property and Residual Estate: I bequeath the remainder of my estate, property and effects, whether movable or immovable, wheresoever situated and of whatsoever nature to my spouse JANE WILSON.

(6) Alternate Beneficiaries: Should my spouse not survive me by thirty (30) days then I bequeath the remainder of my estate, property and effects, whether movable or immovable, wheresoever situated and of whatsoever nature to:

Name: MICHAEL WILSON (SON)

Bequest: 50% of remaining estate.

Name: AMY WILSON (DAUGHTER)

Bequest: 50% of remaining estate.

(6.1) Should any of the beneficiaries named in (6) not survive me by 30 (thirty) days I direct that the non-surviving person's share goes to the remaining beneficiary.

(7) Special Requests:

(7.1) I direct that my Final Arrangements Document be executed upon my death.

(7.2) I direct that details of this document are not to be shared publicly or online.

(8) General:

(8.1) Words signifying one gender shall include the others and words signifying the singular shall include the plural and vice versa where appropriate.

(8.2) Should any provision of this Will be judged by an appropriate court of law as invalid it shall not affect any of the remaining provisions whatsoever.

(8.3) If any beneficiary under this Will contests or attacks any of its provisions, any share or interest in my estate given to that contesting beneficiary is revoked and shall be disposed of in the same manner provided herein as if that contesting beneficiary had predeceased me.

(8.4) This document shall be governed by the laws in the State of California.

IN WITNESS WHEREOF I hereby set my hand on this 7th day of July, 2020 in the presence of the undersigned witnesses.

JOHN WILSON

As witnesses we declare that we are of sound mind and of legal age to witness a Will and that to the best of our knowledge JOHN WILSON is of legal age to make a Will, appears to be of sound mind and signed this Will willingly and free of undue influence or duress. We declare that he signed this Will in our presence as we signed as witnesses in the presence of each other, all being present at the same time. Under penalty of perjury, we declare these statements to be true and correct on this 7th day of July, 2020.

Witness Name

Witness Name

Witness Signature

Witness Signature

Date

Date

After-Death Data Access

The final consideration in regard to death is the accessibility of your data. When you die, the passwords known only to you also die. This may eliminate the ability to access your documents, media, accounts, communications, and anything else you have protected. For some, this may be intentional. You may not want anyone to be able to access this information, even after your death. For others, it is vital to allow a spouse or other family member complete access to your digital life. This could also apply if you are alive but mentally incapacitated.

Imagine that you control all of the online accounts related to your house, banks, utilities, and aliases within a password manager. You die and your spouse cannot access these details in order to continue payments and maintain your privacy strategy. This can be devastating, especially if nothing is in your true family name. For most clients, I recommend an after-death data access strategy. If you created any of the documents previously discussed in this chapter, you should attach a separate document explaining any components of your privacy strategy which would be needed after your death. This should include the following.

- Passwords required to access any online accounts associated with your home.
- Detailed alias names used for any services or utilities associated with your home.
- Detailed payment processes for any services or utilities associated with your home.
- Detailed access instructions for any financial accounts.
- Detailed access instructions for secured containers (safes).
- Detailed access instructions for any virtual currencies stored digitally.
- Copies of any trusts, Wills, and financial records.

Next, you should consider keeping important accounts active. If you have a premium email subscription, it must remain funded in order to keep the account active. It may not matter that your spouse has all of your passwords if your account has been disabled. Enabling auto-pay to a valid credit or debit card may get you through a couple of years past your death, but the expiration on the funding source is a valid concern. Some providers allow you to add funds to an account before expiration and any renewals simply withdraw from that source.

If you adopt a custom email domain strategy, you might want to ensure that the domain does not expire after your death. Fortunately, most domain registrars allow you to renew for multiple years. I keep my primary email domain renewed for ten years at all times. Even when it has eight years remaining, I can top it off to the full ten years. If your domain expires, you have two issues. First, your email is no longer forwarded and your family may not be able to monitor monthly messages for answers about accounts and services. Next, any password resets or account verification emails will not be forwarded to your email provider. This can

prevent access to various accounts and block your family members from proving they have authorization to act on your behalf. Losing access to email can be a catastrophe.

In 2020, the spouse of a deceased client contacted me out of desperation. Her husband had titled the home in the name of a trust and all utilities were automatically paid out of an LLC checking account. When she decided to sell the home, she realized she had never seen the trust details. She had no idea of the identity of the trustee used during the purchase. She could likely retrieve a certification of trust from the county or title company, but this would never suffice for the documents required during closing.

I was able to provide the last known signed and notarized documents which I had helped her husband create at the time of purchase. This is one reason I securely store copies of all client documents offline. We were able to determine that she had the authority as the Grantor in the event of her husband's death. This allowed her to reassign herself as trustee and complete the sale. Without it, I do not know what would have happened. Make sure that you have a way to deliver all important documents to your family after death.

These are only a few considerations. Think about what information will be needed when you die. Making this content easily available may seem risky. What if this data gets into the wrong hands? This is a very valid concern. You should be creative and cautious in how you disseminate these details. Some may include written information in the same envelope as their legal documents within a safe. I take it to another extreme.

I created a text document which includes every detail needed to reconstruct my complicated digital life and understand my use of aliases, trusts, and LLCs. It is encrypted within a VeraCrypt container and copied onto USB devices held by my two beneficiaries. My attorney possesses a password which is to be given to each beneficiary only upon my death. The beneficiary can use that password, followed by the serial number of the USB drive to unlock each VeraCrypt database. The serial number is visible on the device itself and included in a text file on the drive.

This way, the attorney has no access to the data, and each beneficiary requires cooperation of the attorney in order to access the content of the data they hold. Since each beneficiary has the ability to access the data without the other, there is a bit of redundancy in my plan in case one should lose the data or precede me in death. Every few years, I update the content on each USB drive in order to stay current. It makes for an awkward visit. I hope this page has generated some ideas on how you will tackle this dilemma.

Dual Citizenship

On rare occasions, I hear from a client that he or she wishes to obtain dual citizenship. This provides a second passport in your true name from a country outside of America. Dual citizenship is completely legal, but a huge hassle. There can be several legitimate reasons to desire a second passport from another country, but they are mostly obtained for the “cool” factor. If I were forced to identify legitimate needs for dual citizenship as an American, I would provide the following three reasons.

Travel: A second passport can protect you from travel limitations and provide more visa-free travel. Visa-free travel is the ability to enter a country without obtaining a visa in advance. If you have a U.S. passport, you need to obtain a visa to travel to places such as China. This can become an expensive and time-consuming task if travel is frequent. If you had a passport from Grenada, a visa is not required to enter China from a country other than the U.S. These scenarios are rare, but legitimate for some.

Investments: Many countries refuse to allow Americans to invest within their territory. This is often due to strict American banking laws which requires citizens to report offshore accounts. Foreign banks simply do not want to deal with you or the IRS. A foreign passport can break through these barriers and allow investment. I do not get involved with clients in this situation. It almost always leads to some level of tax avoidance.

Safety: Having more than one option means you don’t belong to a single government. If things become unsafe in America, and we find ourselves in danger simply being present, you can immediately and effectively take yourself and your family out of harm’s way. While unlikely, options are always a good idea. My clients who desire a second passport usually fit mostly into this category.

There are three main strategies to obtain a second passport, which are ancestry, time, and money. All of my clients who have expressed interest in dual citizenship have chosen the easiest option, which is money. If you have enough of it, you can buy a passport from one or more of many countries. I have one client who collects them like baseball cards. Let’s first take a look at the three avenues to dual citizenship, in order of most affordable to most expensive.

Ancestry

Obtaining a second passport usually requires either a lot of time or a lot of money. If you have the good fortune to have parents, grandparents, or in some cases, even great-grandparents from specific countries, a second citizenship can be easily and inexpensively obtained. If you have ancestors from Italy, Poland, Ireland, Germany, England, France, Portugal or Estonia, you might be entitled to citizenship based on ancestry. This means you can get a second passport in a very short time, and at very low cost. I always encourage clients to explore their family tree and identify any easy routes first.

Time

Most countries provide an option for naturalization through residency. However, the conditions vary with each country. Consider the following three factors.

- How long must you be a resident in order to be eligible to begin the application process for naturalization?
- How difficult is it to obtain residency? There are many countries eager to take in hard-working individuals, while others scrutinize and deny most applicants.
- Do you actually need to physically live there? Many countries' naturalization regulations require an applicant to spend the majority of time in that country. If you spend too much time out of the country, you render yourself ineligible for citizenship. Some countries have very minimal requirements for the length of time you must be physically in the country.

Money

Finally, the easiest option. If you have enough cash, you can often "buy" your dual residency. In previous decades, enough money would guarantee you a passport within weeks, without any investment or time requirements. In some rare cases, a \$5,000 "donation" to the country generated a passport that same day. Those deals are no longer available, and the theatrics have changed. Countries now often require large investments while some still accept pure donations. As I present each country's options, I clearly display the outright fee you can pay in order to quickly bypass the lengthy application process for traditional naturalization.

Residency vs Citizenship

If you are not eligible for a second passport through ancestry, time, or money, the next best option is to obtain a second residency. It gives you the same benefit of always having a place to go, and it can potentially help you obtain a second passport within a few years through naturalization. Residency should not be confused with citizenship. Citizenship provides you an official passport which can be used for transportation. Residency simply grants you the authority to reside in the country. Residency is often a large role in the path toward citizenship.

The following pages explain the possibilities for obtaining a second citizenship for many of the countries which allow it. In order to avoid preference, or expose my own interests in this privacy strategy, I have listed them in alphabetical order. Please note that foreign politics change rapidly, and this information could become outdated quickly. While there may be additional countries which allow this and are not listed here, I present those which have a lengthy track record of positive experiences. There are many online scams surrounding “too good to be true” options which should be avoided. Each country summary ends with two considerations, as displayed below.

Cost: The average fee (USD) you will pay to obtain dual citizenship, instead of time.

Time: The amount of residency time required to apply for citizenship, instead of a fee.

Antigua and Barbuda

Antigua previously offered an affordable economic citizenship program, and recently reinstated it with much higher costs. There are now three options under Antigua’s program.

- Pay \$250,000 as a donation to the National Development Fund, as well as approximately \$50,000 in legal and other fees.
- Purchase government-approved real estate valued at \$400,000 or more, and hold that real estate for at least five years. You must also pay nearly \$100,000 in legal and government fees per adult, and about \$50,000 per child.
- Invest in a local business or businesses with a minimum investment of \$1.5 million.

Cost: \$300,000 or \$1.5M investment

Time: Not Applicable

Argentina

An Argentine passport allows visa-free travel throughout all of Europe, including Russia. However, Argentine passport holders must have a visa to enter the U.S., Canada, and Australia. Argentina’s nationality law has been unchanged since 1869 and states that one can qualify to become a citizen after only two years of residing in the country. Any residency visa

qualifies you for this. Similar to Chile, the easiest options are “rentista” or retiree visas, which require you only to prove a certain amount of monthly passive income. In Argentina, in order to qualify for the rentista visa you need to demonstrate a minimum of \$1,000 per month in passive income, which needs to be transferred to an Argentine bank account in your name. The rentista visa is a temporary one-year visa. It can be extended in one-year increments. It is best to initiate the residency process while in Argentina, not as a consulate abroad, which would complicate matters unnecessarily. Once you have your residency, you should spend at least six months of the year in Argentina for both years. After two years, you may apply for naturalization. Upon application you will need to demonstrate an intermediate level of Spanish language proficiency. The language test is very informal and “friendly”, usually consisting of a short conversation.

Cost: Living expenses

Time: 2 Years

Belgium

Belgian citizenship is quite valuable as a gateway to the European Union. It has some great options for first gaining residency, and once you become a resident you can apply for naturalization in 5 years. The most appropriate way to obtain residency in Belgium, and eventually citizenship, is to create a company in Belgium and apply for the professional card residency. You could also hire yourself from your company and apply for a work permit. This requires the services of a legal professional to assist you through the process. Obtain a residential address by renting or purchasing a home. Once you have the address, register it with the local city hall. Stay at that residence for the initial police check, which usually happens within two weeks and likely won’t be repeated during the course of the visa. This makes you a resident of Belgium. After two years, apply for renewal, then renew every 5 years. You are eligible to apply for naturalization after five years. You can then go to the local municipality to state your intention of becoming a naturalized Belgian citizen. They will inform you of the documents necessary for application. In order to become naturalized, you do not need to physically live in Belgium full-time. The Belgian government has no way of knowing whether you are spending your time in bordering countries. However, you do need to spend a “reasonable” amount of time there each year and show that you are a member of the community.

Cost: Living expenses

Time: 5 Years

Chile

A Chilean passport allows you to travel to 150 countries visa-free. It is one of only two travel documents that enables you to travel to all G8 countries visa-free. This includes the U.S., Canada, and Russia. It requires approximately five years of continuous residency, first

temporary, followed by permanent residency. For individuals with established income and assets, the easiest option is called the rentista visa. To apply for this visa, you need to prove that you have income from investments held overseas. The easiest path for most clients is a lump-sum held within a bank account which pays interest. After nine months on the rentista visa, and having spent at least six months in Chile, you can apply for permanent residency. The six months do not need to be consecutive and can be accumulated over the course of one year. When you apply for naturalization, your case is best supported if you can show some legitimate ties to the country. This includes the ability to speak basic Spanish and demonstrating that you are involved in the local community.

Cost: Living expenses

Time: 5 Years

Cyprus

A Cyprus passport is less attractive after the financial crisis of 2013. You have two options, both of which require a large amount of money.

- Invest 2,000,000 euros into Cyprus businesses, with at least 500,000 euros of that amount as a donation to the government's Research Fund. If you don't want to make a donation, you must invest 5,000,000 euros.
- Deposit 5,000,000 euros in a Cyprus bank for three years.

Cost: \$2M - \$5M Investment + \$500,000 donation

Time: Not Applicable

Dominica

This Caribbean country's passport program only offers a donation option. This means your entire "investment" will not be recovered. The most affordable passport program options cost approximately \$130,000 for an unmarried applicant.

Cost: \$130,000-\$150,000

Time: Not Applicable

Grenada

Grenada offers a real estate investment option that requires a \$500,000 investment. However, that investment must be made in only one government-approved development, and obtaining a second passport in Grenada comes with a residency requirement. You must actually reside there most of the year.

Cost: \$500,000 investment

Time: Not Applicable

Malta

Malta was a great option until their corruption was exposed. An amendment passed in 2013, legally granted eligible persons EU citizenship via Malta by investment in the Malta Individual Investor Program. To be considered eligible for the Malta citizenship scheme, the applicant must be at least 18 years of age and meet several immigration requirements. The Malta citizenship by investment program has some of the strictest due diligence standards of any immigrant investor program in the world. Applicants must have a clean criminal record and must provide a police certificate before they will be approved for European citizenship. All individuals and families applying to the Malta Individual Investor Program must make a significant non-refundable contribution to the National Development and Social Fund set up by the Government of Malta and run by a board of trustees. The following contributions must be made within four months of being issued a Letter of Approval in Principle:

Main applicant - \$650,000

Spouse - \$25,000

Minor children - \$25,000 to \$50,000 each

Dependent parents & grandparents - \$50,000 each

Applicants must commit to retaining an immovable residence in Malta for a minimum of five years. This can be done by either buying a property in Malta for at least \$350,000 and maintaining ownership for five years, or by leasing a property for five years or more with a minimum annual rent of \$16,000. Applicants are also required to invest at least \$150,000 in government approved financial instruments such as bonds, stocks, and debentures that benefit the nation. Upon purchasing real estate or entering a property lease in Malta, investor citizenship candidates are issued a Malta identity document called an eResidence card. This signifies the commencement of their residency in Malta and also demonstrates the candidate's genuine link with the country. Twelve months after an applicant has established residency in Malta, he or she will be granted citizenship. Maltese law defines residence as "an intention to reside in Malta for any fiscal year, usually evidenced by a stay of a minimum of 183 days or by the purchase/rental of property together with a visit to Malta".

Cost: > \$1,000,000

Time: Not Applicable

Panama

Panamanian residency is one of the easiest in the world to obtain. After five years of residency, you are eligible to apply for naturalization. A Panamanian passport offers you visa-free travel in 125 countries. This passport is attractive for many because there are exceptionally low requirements for the amount of time you must be present in the country. This makes for an excellent "Time" option, in which you do not technically need to spend time in the country.

A second benefit is the country's territorial tax system, which means that Panamanian residents and companies only have to pay local tax on their Panamanian-sourced income. As long as your income is earned outside of Panama, it is not taxable by Panama.

The easiest residency option is through the Friendly Nations Visa, which applies to nationals of more than 40 countries, including the U.S., Australia, most European countries, Israel, Japan, Hong Kong, South Korea, Singapore, South Africa, and several Latin American countries. Citizens of any of these countries can obtain residency in Panama extremely easily by merely demonstrating "economic activity" in the country. This does not mean that you necessarily need to conduct any business within Panama. Instead, you can satisfy this requirement by registering a Panamanian corporation and making a reasonable deposit at a local bank. Once you submit your residency application, you are free to leave the country and come back a few months later to collect your documents and ID card.

You do not need to physically reside in Panama. Panama's immigration code only requires that the visa be renewed after two years. Aside from that, you do not need to spend any time there. After five years of residency, you are qualified to apply for naturalization. As always, your naturalization case will be much smoother if you have basic knowledge of the Spanish language and you can demonstrate involvement in Panama's business and social life.

Cost: Living expenses

Time: 5 Years

St. Kitts & Nevis

I first learned about this option when reading the book *Emergency* by Neil Strauss. He documented his efforts to obtain this passport, which was surprisingly easy. Things have changed. The popularity of this program has introduced much stricter rules and inflated fees. This is the longest running second citizenship program in the world and has been in operation since 1984. To get a St. Kitts passport today, you must choose one of two options:

- Make a donation of \$250,000 or \$300,000, depending on your family size, to the government's Sugar Industry Diversification Fund. This fund was established to help the workers who lost their jobs when the sugar industry became unviable. This is a gift to the country and not an investment.
- Purchase at least \$400,000 in "government approved" real estate. These are extremely overpriced and held specifically for wealthy subjects desiring dual citizenship. While you technically own the properties, there is very minimal chance of ever recouping the cost.

Cost: \$250,000 - \$400,000

Time: Not Applicable

Renouncing Citizenship

In 2018, I had a client who insisted on renouncing his U.S. citizenship. I never recommend this, but his political reasons outweighed my concerns for him. He was confident in his decision, and was ready to proceed with or without my assistance. He had recently acquired a secondary citizenship in one of the countries mentioned here. This is not technically required in order to renounce citizenship, but heavily recommended. If you have no other country of citizenship, you would become stateless. It would be very likely that your request to renounce would be rejected.

Once he had his new citizenship in order, he traveled to that location. You should always schedule an appointment with the U.S. embassy or consulate of the location of your secondary citizenship. During the first meeting, diplomatic officials ensure that you are not renouncing your citizenship under duress. You will also need to complete a DS-4079 form (available at <https://eforms.state.gov/Forms/ds4079.pdf>). The second appointment requires you to read an oath in which you state your desire to renounce citizenship. Your documents are then sent to the U.S. State Department, which reviews the paperwork and makes a decision on your case within two months. If approved, you will receive your Certificate of Loss of Nationality. After renouncing your citizenship, you no longer pay future U.S. income taxes, and you will not need to report income unless you invest or do business in the country. However, you are required to file a final tax return covering the time between January 1 and the day you renounce. If your average annual net income tax in the past five years was \$162,000 or more, or if your net worth is more than \$2,000,000, you may have to pay an exit tax. The standard fee for renouncing citizenship is currently \$2,350. The exit tax can be 30% of your wealth. Again, I never recommend this. Most people who request information about renouncing citizenship eventually decide it is not worth the hassle and risk. Even if you choose to leave the country and live abroad, possessing a U.S. passport is a luxury that many spend years to acquire.

Expatriate

If you believe you need a second citizenship, I encourage you to first consider becoming an expatriate (expat). An expatriate is someone who lives in a different country other than where they are a citizen. In general, expatriates are considered to be people who are residing in their host country *temporarily*, with the ultimate intention of returning home at a later date. However, many expatriates leave their home country and find they can experience a better life abroad. For this reason, many of them never return home, but do not necessarily require a second citizenship. More details, including popular places for expats, can be found at www.expat.com. You might also consider the following tactics which allow extended residency within specific Caribbean countries under a remote work program.

Remote Work Dual Residency

Many clients desire a second citizenship in order to obtain another passport and permanent residency whenever desired. That is overkill for most. In 2020, I saw an abundance of Caribbean countries offering a quick residency option to those who can work remotely. The COVID-19 pandemic was devastating for countries who rely heavily on tourism funds. In effort to bring in money to hotels, restaurants, and other businesses, many countries loosened their restrictions on long-term stays. The following currently offer work residency programs.

- Antigua and Barbuda
- Bahamas
- Barbados
- Bermuda
- Cayman

While each country has their own rules, the following is typically required for participation.

- Application fee ranging from \$500-\$1700
- Valid local health insurance
- Proof of income ranging from \$50,000-\$200,00 annually
- Air travel
- Two weeks of quarantine at hotel or other lodging
- Long-term lodging throughout stay
- Bank statements and proof of funds letter
- Proof of identity
- Criminal record from FBI or local agency

Most islands offer an immediate two-year residency allowance with the option to extend at expiration. None of these islands currently offer citizenship to those who participate in the remote work program, but that could change. By the time you read this, the pandemic may be over and these islands may have withdrawn the program. If another pandemic arrives, these may be places of interest to you. I had experience with this program in late 2020. It works well if you are self-employed or own your own company, and can conduct business remotely over the internet. It does not work well if you need to leave and return often. At the time of this writing, an additional 14 days of quarantine are required every time you return. I talked with many colleagues and friends who participated in these programs. While the sun and weather were wonderful, “island fever” is a real threat. This is the realization that you are stuck on an island without any easy way to return to your home country to visit others. I witnessed a huge sigh of relief once the COVID-19 vaccine was available and remote workers could go home.

Birth Tourism

There is an additional path to citizenship that I have not yet mentioned. Being born within a country that honors the “*jus soli*” principle, which means “right of the soil” in Latin, can immediately generate dual citizenship. This means that children born in these countries are granted citizenship, regardless of the nationality or immigration status of the parents. In some countries, being born within the borders of the country is enough to automatically be granted citizenship, even if the parents are there as tourists. Countries with unrestricted *jus soli* laws include the following.

Antigua & Barbuda	Chile	Guyana	Peru
Argentina	Costa Rica	Honduras	Saint Kitts & Nevis
Azerbaijan	Cuba	Jamaica	Saint Lucia
Barbados	Dominica	Lesotho	Saint Vincent
Belize	Ecuador	Mexico	Tanzania
Bolivia	El Salvador	Nicaragua	Trinidad and Tobago
Brazil	Fiji	Pakistan	United States
Canada	Grenada	Panama	Uruguay
Chad	Guatemala	Paraguay	Venezuela

In some other countries, one can only obtain citizenship for the child if certain additional requirements are met, such as that at least one parent is a citizen or permanent resident, or that at least one parent was born in the country themselves. Notable options include the following, and are not usually recommended.

Australia	Dominican Republic	Hong Kong	United Kingdom
Chile	France	Ireland	
Colombia	Germany	New Zealand	

While it is too late for you to choose where you are born, you can make preparations for your child to possess dual citizenship. Some countries, such as Brazil and Panama, allow the parent of a child born on the soil to go through the expedited naturalization process. I will explain more on that in a moment. First, let's consider reasons why one might choose birth tourism as a privacy strategy for a newborn child.

Immediate dual citizenship: Many people strive to obtain dual citizenship for themselves. It can be very costly and can take years to accomplish. With most birth tourism, dual citizenship is immediate for the child. This can be very enticing for parents with an interest in this topic.

Healthcare: Every year, thousands of babies are born in the U.S. to mothers from China. Parents do this to obtain American citizenship for their children. They spend tens of thousands of dollars to hire agencies that help arrange their trips to the U.S. because America's healthcare system is desired. Many people in China do not trust their domestic medical system, which is underfunded and overburdened. Under-the-table payments to doctors in the form of "hongbao" (lucky money) are exchanged as a way to skip long patient queues or ensure patients are treated well. Canada is also experiencing high rates of birth tourism because of this issue.

Education: Many citizens of countries with poor education systems crave a better option for their children. Being born in most Western countries entitles the child to education choices which would never be present in their parents' home countries.

Travel Restrictions: This was previously explained. Parents that desire less restrictive travel for children throughout their lives can use this strategy to bypass visa requirements from their home country.

Child Limits: Some countries, such as China, impose limitations on the number of children allowed per family. While these laws have been relaxed in recent years, they still exist. Births outside of these countries can bypass restrictions. In China, this requires parents to exclude their children from the Chinese national household registration system, which can present other problems. Overall, this strategy is not usually justified.

Parental Citizenship: This is the primary reason for privacy-conscious parents to explore birth tourism. The child born on foreign soil is often referred to as an "anchor baby". Parents intentionally give birth in a specific country in order to possess a child with citizenship in that country. The intention is to use this connection in order to gain their own citizenship. I will focus only on this strategy for the remainder of this chapter, as it is the most applicable to extreme privacy. Let's walk through a typical scenario, which is loosely based on my experiences with two separate clients, both American citizens. I cite Panama as the desired country of secondary citizenship, but you could substitute many of the "jus soli" countries in its place. The following is presented as a checklist of considerations.

- **Decision:** When a person is expecting a child, there is obviously a small window of time to consider if secondary citizenship might be beneficial to the child's future. I urge parents to consider all options, including eliminating this strategy completely.
- **Timing:** Traveling days before a birth due-date is risky. Giving birth on a plane does not accomplish anything. For those considering a foreign birth, I recommend arriving at least a month before the due-date. This gives time to become familiar with the area without a sense of urgency.

- **Birth:** After the child is born, citizenship of the country is immediate. The birth is reported locally and a birth certificate is issued. In this scenario, the child is a citizen of Panama, regardless of the parents' nationalities.
- **Documentation:** Aside from the official birth certificate, a passport can be requested on behalf of the child.
- **"Home" Citizenship:** If the parent(s) are American citizens, the birth should be reported to the U.S. while still abroad. The 2001 Child Citizenship Act (CCA) outlines the requirements with "a child who is under the age of 18, was born outside the U.S., and has at least one U.S. citizen parent automatically acquires U.S. citizenship upon entry into the country as an immigrant".
- **"Home" Documentation:** The parent can request a Certificate of Citizenship and U.S. passport for the child. The child's parents should contact the nearest U.S. embassy or consulate to apply for a Consular Report of Birth Abroad of a Citizen of the United States of America (CRBA) to document that the child is a U.S. citizen. If the U.S. embassy or consulate determines that the child acquired U.S. citizenship at birth, a consular officer will approve the CRBA application and the Department of State will issue a CRBA, also called a Form FS-240, in the child's name. According to U.S. law, a CRBA is proof of U.S. citizenship and may be used to obtain a U.S. passport and register for school, among other purposes. This should be submitted, authorized, and received while still abroad. If desired, the entire family, including the child with dual citizenship, can safely travel back to the U.S. legally.
- **Parental Application:** The parents can now apply for fast-tracked secondary citizenship. In our example, Panama's President signed a new law allowing foreigners who gave birth to a child in Panama within the last five years to qualify as permanent residents. Many other "jus soli" countries offer this, but the time, expenses, and requirements vary greatly.
- **Basic Requirements:** In Panama, and most other countries, a nationwide criminal police record of both parents must be filed from their home country's national police force. For U.S. citizens this will usually be from the FBI. If one or both parents have lived in Panama without having left the country for a minimum of two years, he or she can obtain the criminal background report from the Panama police (Department of Judicial Investigations "DIJ"). You must also provide an original birth certificate for the child from the Panama Civil Registry. Finally, you must file a letter of responsibility signed by a Panama citizen. This is usually completed by an attorney.
- **Financial Requirements:** Most countries require proof of economic solvency, such as a letter from a Panama bank displaying adequate funds of the applicants. Countries want to ensure you will not further drain their resources for citizens.

- **Costs:** Our scenario with Panama is on the low end of costs. The average expenses per parent include a \$1,050 application fee for the immigration department, \$150 for the permanent residency carnet (ID card), and up to \$2,000 in legal fees. The high end for other desired countries can be over \$20,000 per parent.
- **Time:** Obtaining residency in Panama is almost immediate and full citizenship can take up to a year. Other countries can require up to three years for full citizenship for parents of a child born locally.

I hope I did not make this process sound easy. There are always numerous unexpected hiccups when governments move slowly or scrutinize applications. Overall, I do not recommend this privacy strategy for most people. The following explains some complications to consider.

- **Same-Sex Parents:** Many countries do not recognize marriages of same-sex couples, and may exclude residency and citizenship options for anyone who is not biologically connected to the child. I have seen this in the U.S. In one scenario, a couple experienced hurdles after a birth in London. A child was born via surrogate to a male same-sex couple from the U.S. The baby's parents were married and both were U.S. citizens, but the sperm-donating parent was originally born in Britain. Shortly after birth, the U.S. State Department issued a letter informing the couple that their child was not a citizen of the U.S. at birth. The parent with a genetic attachment to the child had not lived long enough in the U.S. as a citizen to pass his citizenship to the child. The other parent, who was a natural born U.S. citizen, could not establish a "blood connection" to the child. According to the principles of "jus soli", the child was an "alien" to the U.S.
- **Government Scrutiny:** Many countries, including the U.S., Canada, U.K., and Australia, are scrutinizing babies born during birth tourism, and proposing laws to prevent it. I do not recommend this tactic as a way to gain citizenship in these countries.
- **Healthcare:** While this was previously mentioned as a benefit for some expectant parents, it can also be an undesired consequence. Some of the countries which allow this do not possess quality healthcare. You may find yourself in a very uncomfortable situation outside the expectations of healthcare in your home country.
- **Stateless Child:** In a worst-case scenario, you may find all of your effort wasted and your child in a "stateless" condition. The country of birth may not recognize the child as a citizen and your home country may not allow entry of this undocumented foreign person. Always do your homework and seek legal help local to the target destination.

Summary

Name changes, dual citizenship, secondary residency, and birth tourism are extreme privacy tactics, but required for some targeted clients. I cannot think of a more powerful privacy strategy when trying to avoid America's surveillance than to simply leave. I close with a warning. Secondary citizenships often carry risks. Some countries require mandatory military enlistment for all citizens. Some apply inflated taxes on secondary citizens. A few are always at risk of financial ruin, and any investments could be lost. I try to discourage clients from these methods unless absolutely necessary. The grass is not always greener on the other side. Also, I can speak from experience when I report that secondary citizenship does not bode well for a security clearance renewal.

CHAPTER FIFTEEN

DAMAGE CONTROL

If you applied most of the previous privacy strategies toward your life, you should be in good shape, for now. Around every corner is an invasive threat toward your privacy. Data mining companies, marketers, and government entities continue to want your information. It has extreme value in our data-obsessed world. If you want to keep the level of privacy you created, you must put forward effort to maintain it. This chapter presents many considerations for staying private and secure after all of your hard work.

My first advice is to eliminate all potential online privacy threats such as social networks. There is no way to use Facebook, Instagram, Snapchat, and other similar services anonymously. They all possess numerous technologies which attempt to identify you, your location, and your online habits. If you absolutely must use social networks, only use them within your web browser. Never install mobile social network applications on your devices. Viewing Facebook through a web browser gives you some control over which information it can access. Opening the Facebook app provides a deeper level of access to your device's data.

Hardware technologies are also a constant threat. It is becoming much more difficult to purchase various home electronics without jeopardizing your privacy. Consider the following common purchases and associated concerns.

Home Assistants: Amazon Echo and Google Home devices have seen a surge in popularity and adoption. These are the small devices that listen for you to say “Alexa” or “Hey Google” while in your home in order to assist you with daily tasks. Most users of these devices allow them to conduct searches, display videos, or place orders online with only a voice command. I will never allow these devices in my home. A quick search online reveals numerous reports which provide sufficient evidence for my concerns. Amazon admits that numerous employees listen to you through these devices and that they keep the recordings forever. Google is more tight-lipped, but I expect the same.

Smart Doorbells: The Ring doorbell is now owned by Amazon while the Nest option is owned by Google. These have become a trophy of sorts displayed at the front doors of many households. These devices stream video and audio over the internet from your home. If a stranger is at your door while you are at work, you receive a notification and can interact as if you were home. I completely understand the security value of such a device. However, my privacy concerns outweigh the benefits. These devices are invasive to your neighbors across

the street and provide potential hacking attempts since they are connected to the internet. In 2021, Ring announced it would start allowing your neighbors to connect their devices to your Wi-Fi without consent. I could never imagine allowing this in my home.

Televisions: Practically every modern TV available today has embedded Wi-Fi and software which reports usage back to the manufacturer. Some possess front-facing cameras. This is extremely invasive. Most people express little concern for this, as they never connect the TV to their home Wi-Fi, which is encrypted with a password. This is not enough to prevent connection. Some TVs are configured to connect to any open Wi-Fi, such as a neighbor or coffee shop. You could find the wireless adapter and unsolder it from the board, but you would take a high risk of ruining the TV. My preference is to purchase monitors instead of televisions. Since I connect my TV to a media center and amplifier with speakers, a large computer monitor is plenty for my needs. You may pay a slight premium for this, but I find it justified. If you are not convinced, please consider the following.

Samsung is one of the most popular smart TV manufacturers. During Christmas season of 2019, they made a strong marketing push in reference to their “intelligent” TVs which could control home automation; learn to know your interests; and listen for voice activation through mandatory internal microphones (which are always enabled). They also promoted use of internal cameras (which are always enabled and facing the viewer) and the ability to control your TV from any smartphone. I find all of this invasive to our privacy, but their own privacy policy confirms why I will never have one of these devices in my home.

“...the IBA Service will collect information about your TV viewing history (including information about the networks, channels, websites visited and programs viewed on your Samsung Smart TV and the amount of time spent viewing them) and Samsung Smart TV usage information (such as how long and often you use the apps on your Smart TV). We may use automatic content recognition (ACR) and other technologies to capture your TV viewing history. We also may obtain other behavioral and demographic data from trusted third-party data sources...”

The ACR feature referenced in their policy is the ability for Samsung to collect screen captures of your current viewing, transmit them to Samsung networks, and analyze the content. This could include public channels, streaming services, private content played through external media, photographs, home movies, and anything else which may be present on your screen. Yes, even pornography can be copied and transmitted to Samsung. Do you view personal slideshows of family photos on your smart TV? Technically, those can be collected and transmitted back to the manufacturer. Some online privacy enthusiasts have reported that Samsung transmits data through over 200 connections within ten minutes to various subdomains of samsungelectronics.com. Is this legal? Yes, we agree to their terms of service by simply using the product. What can you do?

The first step is to avoid these features when possible. Never connect your TV to any Wi-Fi. If still concerned, create an open Wi-Fi access point and monitor the TV and router log to see if a connection was made to the open network. If you know your TV has no connection to the internet, you are probably fine. Cover any cameras with privacy stickers as mentioned earlier. Navigate through your on-screen controls and disable everything possible. This does not prevent communication attempts, but should lessen the threats substantially.

Lack of connections will also disable desired features such as Netflix and other premium streaming services. I always recommend a separate media server for these options, such as a Roku, Apple TV, or FireTV device. These have their own privacy issues and concerns, but do not send data to your television manufacturer. Each possesses their own version of ACR, but also allows you to disable the option completely. Personally, I prefer a Kodi media server. This option requires a bit of work to set up, but affords more privacy. The details of a Kodi installation exceeds the scope of this book, but online tutorials are abundant.

My policy is to avoid all unnecessary internet-connect devices as possible. My refrigerator does not need to be online. I prefer to control my thermostat with my hand while in my home. Every time you provide internet access to hardware in your home, you now have an additional attack surface. If you do not constantly apply security patches to these devices, you risk immediate exposure once a new vulnerability is published. It is easier to avoid the problem completely by minimizing the number of internet-connected devices. Even if you think you have a low-tech home, it is still vital to scan for vulnerabilities. I conduct two types of audits often within my home and the homes of clients. The first is to discover any connected devices which may be unauthorized. The second is to scan for open Wi-Fi which could unintentionally be used to transmit data from any devices desired to be offline.

Scanning Devices: Since I possess a pfSense firewall as explained previously, it is quite easy to identify the devices on my network. After logging in to pfSense, navigate to “Status” > “DHCP Leases”. This screen displays every device on the network which has been issued an IP address from pfSense. This should include any devices connected through your wireless router, as long as you disabled DHCP from that device and rely on pfSense to provide the addresses. If you see anything with an unusual name, investigate.

Scanning Open Wi-Fi: I first reset the network connections on my iPhone (Settings > General > Reset > Reset Network Settings > Confirm). This removes any known Wi-Fi connections. I then analyze any networks without a lock icon in my Wi-Fi connection screen (Settings > Wi-Fi > Networks) while I move around my property. If I locate any open connections which I control, I make the necessary changes. If I find a neighbor with open Wi-Fi, I politely tell them about the risks associated with this behavior. My goal is to simply eliminate any open Wi-Fi which could be used by any device without my authorization.

Kindle and Other E-Readers

You may be surprised to see a section devoted to electronic book readers, such as the Kindle. After all, what could be invasive about reading an e-book? You may be surprised. If you are using a Kindle, Amazon collects and stores the following details about you in your profile, and then shares it with third parties (with your consent from the Terms of Service with which you agreed when activating the unit).

- All books which you have purchased through the device
- All books which you have read through the device
- All books which you have searched from the device
- The last page read of any book in your account
- Any annotations, highlights, or markings within all books
- Speed at which you read any book
- Device language setting
- Wi-Fi and Bluetooth connections
- Estimated locations
- Signal strength
- Times and dates of usage
- Device log files

Some will argue that this is not a big deal. Those people probably did not make it this far into the book. I believe that this is a very big deal. Per the Electronic Frontier Foundation (EFF), this data is shared upon request with law enforcement, civil litigation attorneys, and other Amazon services. If you are involved in a lawsuit, your reading habits, including the date and time that you read a specific chapter, are available to the case. If that happens, this can become public record. Imagine that you are in a child custody dispute or a bitter divorce. If you have been reading books about privacy and security, moving to a foreign country as an expatriate, or growing cannabis, these titles may be used to paint you as shady or unfit. It may be argued that you were reading privacy books to conceal an affair. Your interest in a book about living overseas may be construed as you planning to flee the country to avoid child support obligations. A book about cannabis may be used to make you look like a drug dealer.

Amazon obtains this data when you connect your device to the internet. This happens over the internal Wi-Fi or cellular connection within the unit. The easy solution is to turn off the connection. However, this is also how you obtain new books and have them sent to your device. I encourage you to withdraw from this type of data collection by using the following techniques. I will assume that you are purchasing a new Kindle, but the steps can be applied to existing units. Please note that only a new Kindle will give you complete anonymity. Any existing device already possesses your personal information.

- Purchase a new Kindle from Amazon using a new account created in an alias name. Pay with a masked card for added privacy. Never attach this account to your real name or home address. Ship the device to your CMRA Box or Amazon Locker. Register the device with this account and use any alias name for the Kindle.
- Turn the device on while outside the range of any public Wi-Fi. This could be in your home if your wireless router is secured with a password. Immediately place the Kindle into airplane mode which will disconnect any wireless connections. Never disable airplane mode.
- Order any books for this device from the same Amazon account which was used to purchase the Kindle. The books you purchase will only be accessible on this specific unit. Change the default option of “Deliver to Kindle” to “Transfer via Computer”. Your Kindle will be listed on the following screen. Select “Deliver to”.
- A file with the extension of AZW will be downloaded to your computer. Connect your Kindle to your computer via a USB cable. You should see your Kindle listed as a new drive. Copy and paste the book into the Documents folder of the Kindle. Unplug the device and you can now read this book without invasive tactics.

If the Kindle never leaves airplane mode, you will not share any data from the device. Furthermore, the Kindle cannot retrieve new advertisements to place on your home screen. If your device has never touched the internet, there will never be any ads. Amazon will know the books that you have purchased, but will not know who you are. They will not know the details of your reading and annotating. They cannot target you with ads similar to books that you like. If you plan on purchasing a Kindle, I recommend creating a new Amazon account, and using this account only for Kindle-related book purchases.

Reality Check: We are diving down the rabbit hole of connected devices. We should pause a moment to weigh our risk versus reward. Technology is amazing. The ability to connect our devices to the internet provides wonderful benefit and entertainment. Going too far with disconnections may quickly upset others in your home. Before blindly eliminating internet connectivity from every device you own, consider a conversation with others about the usage and risks.

There might be a middle ground which can gain more privacy while enjoying some of the features of the various devices which you have purchased. I have found that discussing these issues with family before “laying down the law” can create better acceptance of your desires and paranoia. Ultimately, try to involve those who will be impacted by your decisions. While this book is titled *Extreme Privacy*, and my personal application of these tactics are “all or nothing”, every situation is unique. Again, pick your battles wisely.

DNA Kits

Consumer DNA testing kits, such as those from 23andMe and Ancestry.com, provide a detailed map of your genealogy which can include information about your family history and potential diseases to which you could be susceptible. These home testing kits usually require a cheek swab or saliva sample which is mailed to the company. That sample includes your unique genetic code. Most companies will share that data with law enforcement, sell it to third parties, and provide it for numerous lucrative research projects. In the future, it could influence insurance premiums or the ability to obtain insurance at all. I find this frightening.

Many of my clients have asked how to utilize these services anonymously. In simple terms, you cannot. You could order a kit using an alias, masked credit card payment, and anonymous mail drop, but that would be the end of your privacy. Since your DNA sample is unique only to you, it would not take long to discover your true identity. Once another family member submitted a sample using their true name, your sample would be associated due to the genetic lineage. After enough samples were collected from other family members, public data could be used to make the connection from them to you. I strongly recommend avoiding these services, and I encourage your family to do the same. If you think I am being paranoid, research the warning issued by the Pentagon in December of 2019. In an internal memo, Pentagon leadership urged military personnel not to take mail-in DNA tests, warning that they create security risks, are unreliable, and could negatively affect service members' careers.

I suspect that most readers of a book such as this would never want to have a third-party company sequence their DNA, so I will stop the sales pitch for avoiding this technology. Instead, let's focus on what can be done if you have already submitted to this type of testing. We know that your data has already been shared, but you can stop future privacy violations. The following instructions will prevent your stored DNA data from being shared or sold by the top three providers.

23andMe: Log in to your 23andMe account and navigate to the account settings page. Click the “Delete Your Data” option under “23andMe Data”. Download all of your data before you destroy it. If you agreed to have your physical sample saved, it will be destroyed. Some data, including your DNA, gender, and date of birth, will be retained in order to comply with various medical regulations. However, the company will no longer use or share that information.

Ancestry: Log in to your Ancestry account and click the “DNA” tab. Choose “Your DNA Results Summary” and click “Settings”. Choose “Delete Test Results” and re-enter your password. This process will delete your DNA data and prevent you from appearing in any “family finder” results. If desired, you can delete your entire Ancestry account. Your DNA information will be retained for regulatory compliance purposes, but no longer shared or sold.

MyHeritage: Log in to your MyHeritage account and click your name in the upper-right corner. Choose “Account Settings” and scroll to the bottom of the page. Click “Delete Account”. Since MyHeritage labs are CLIA-certified, they will still retain some information about you, but no longer share or sell any data.

Removing this data prevents unauthorized breaches from leaking your sensitive details; private companies from profiting from your DNA; and whatever future risks may surface once companies execute new invasive uses for your genetic profile. I believe we are in the infancy of abuses of DNA data.

Fitness Trackers

Digital health monitoring devices have become very popular. Both Google and Apple understand the value of the mass amounts of personal data captured by these gadgets. It would be very easy to simply state that you should avoid all fitness tracking devices, as they all suck up your personal health data for their own benefit. However, I hear from many people who apply these devices to their daily grind in order to obtain better health and a happier life. Therefore, I provide a few considerations for privacy while benefiting from the features.

First, I absolutely avoid anything manufactured by Fitbit. While some of the older devices have the ability to protect your data, anything purchased recently provides user data to the manufacturer. Alphabet Inc., the parent company of Google, announced its intent to acquire Fitbit on November 1, 2019. The sale closed in 2020. This acquisition provides all collected health data to Google for any use desired. I also avoid anything from Apple. While their business model is hardware sales, and they tout privacy as a fundamental right to its users, they are still a huge company which could benefit from the sale of the health data of millions of customers.

This leaves many independent companies which offer various levels of privacy and security within their devices. I suggest looking for devices which provide the following features.

- Allows you to disable Bluetooth and Wi-Fi
- Enables all features without creating an account with the manufacturer
- Allows you to operate the device without internet access
- Provides enough storage capacity to retain collected information within the device
- Does not require connection to a mobile device

As technology capabilities increase, finding a fitness tracker which respects privacy will become more difficult. I encourage you to research older devices instead of the latest trends.

Financial Data Aggregators

I started my first business in 2006. I began using a service called Mint to organize the finances of the company. Mint was later acquired by Intuit (Quicken) and many new features were added. The online service connected to my bank, downloaded all transactions, and helped me understand the flow of my finances. It relied on a service called Yodlee to keep the connection from my bank to Mint alive. At the time, I never considered the privacy implications of using this type of service.

While I allowed my accounts to be updated daily, third parties were allowed to analyze my transactions and sell that information to practically any other company. Today, there are an abundance of financial data aggregators which will happily facilitate connections to your accounts in order to collect data about you. Quicken, Mint, Yodlee, Plaid, Banktivity, and many others generate billions of dollars of revenue thanks to your data. Consider the following example.

Assume you have a software program, such as Banktivity, installed on your computer. You have paid for the annual service which synchronizes the transactions from your bank account to the software. You can now conveniently keep tabs on your money. However, Banktivity relies on synchronization services from Yodlee, which is now owned by Envestnet. Envestnet receives and analyzes all of your transactions and packages that information for sale to the majority of large financial institutions. Every transaction you have ever made is now in the hands of countless banks, investment firms, and credit providers. This happens without a warrant, since you agreed to the sharing by simply using the product. Today, Envestnet has over 3,000 employees and over a trillion dollars in assets under management.

I encourage you to avoid any service which offers to analyze your financial data or connect to your bank accounts. The convenience does not outweigh the privacy violation. The information collected by these companies could be used to influence insurance premiums, credit scores, or loan applications.

As I write this section, the Wall Street Journal reports that Yodlee is accused of selling consumers' personal financial data without proper consent. Three lawmakers submitted a letter calling on the Federal Trade Commission to investigate the matter. Yodlee, now a unit of Envestnet, currently aggregates data from consumers' financial accounts within 15 of the 20 largest U.S. banks, impacting more than 25 million users globally. The letter partially stated "Consumers' credit and debit card transactions can reveal information about their health, sexuality, religion, political views, and many other personal details. Consumers generally have no idea of the risks to their privacy that Envestnet is imposing on them". I suspect we will soon learn of new ways that companies such as this are violating our privacy.

Unintentional Sharing by Friends & Family

Next, consider your future circle of trust. For many clients, their worst privacy exposure is created by their friends and family. Friends may accidentally expose your home address when they post photos to social networks, and family members will not understand why they cannot send Christmas cards to your home address in your name. This is a delicate consideration which should be discussed with everyone in your household. For my clients with extreme privacy needs, I take a very strict stance. The only people in your life who should know your address should be those who will continuously visit you at your home with your consent. Even then, use caution.

I know this sounds restrictive and harsh. The reality is that every weak link in your privacy strategy is one accidental action away from exposing your hard work. Some clients prefer to visit friends and family instead of welcoming them into their own home. Most provide the PMB address as the only mail contact for cards and letters. You must strongly consider the amount of accurate information you are willing to share and with whom. For many years, I knew people who would temporarily hide any number markings on their home when friends visited. This prevented them from writing down the address and later accidentally exposing it. Today, online maps and GPS eliminate the need for a posted address. Your guests' smartphones are a much bigger threat over human error. I cannot tell you how to approach your own family and friends, but I can disclose a few scenarios that have helped my clients.

When my family visits me at my home, I have a strict faraday bag rule. In my case, I meet them at the nearest town and escort them to my property. I blame poor Google Maps directions and my concern they will get lost. When we meet in town, I collect their phones in a large Faraday bag. They know I am a bit eccentric and no longer question many of my antics. I tell them that they will have a means for communication once we get to the home and assure them that a weekend without phones will be great for all of us. At the house, I provide a community laptop which I have never used with my own accounts. It has a Debian Linux operating system and a Firefox browser (with strong privacy settings). The laptop is connected to my guest Wi-Fi protected by my firewall with VPN. They can visit any website, check any email, and enter any passwords they choose. They can stay connected without exposing my home address through cellular towers or GPS data.

I realize that this will not work for many readers. Most people will refuse to give up their phone and must be connected at all times. I respect their decision and offer to spend time with those people outside of my home area. I am also fortunate that there is no active cellular signal on my property. This was very intentional.

Disinformation

Misinformation is when a person unintentionally provides inaccurate information which causes inappropriate content to be released or replicated. I encourage disinformation. This is when a person intentionally provides false or misleading information with an attempt to create inaccurate data. Disinformation is more valuable to us than occasional misinformation. Disinformation will help make any accurate data about you seem useless inside a stream of completely inaccurate content.

If you have been extremely successful with eliminating your online information and prohibiting new data from being acquired, you may not need disinformation. However, if you have found a few services that display your private data, or simply want to harden your overall security, disinformation may be the perfect solution. Before proceeding, consider whether this action is right for you. Completing these tasks will add more information about you to the internet. Since the information supplied is false, there is little privacy concern. However, this will lead to much more content available about your name.

Many people like this because it creates a difficult scenario when someone tries to locate them. Some people do not like this tactic because it makes their name more visible throughout the internet. Only you can determine if this action is appropriate. Understand that it may be difficult or impossible to remove the false information which you provide.

This section will identify possibilities that you may consider for your own disinformation attempts. They are divided into five specific groups. The options are endless, and I encourage you to email me any great ideas that you have.

- **Name Disinformation:** This will focus on providing many different names to be associated with your real address and real telephone number to make it difficult to identify the true owner of each. This is beneficial for hiding your real name from people or companies searching for information about your address or number.
- **Address Disinformation:** This will focus on associating various addresses with your real name to make it difficult for people or companies to determine which address is your real home.
- **Telephone Disinformation:** This will associate various telephone numbers with your real name to make it difficult for a person or business to identify a valid number to contact you.
- **Business Disinformation:** This will indicate that a fake online business is associated with your true residence. This can dominate online data which may help hide your true details.
- **Death Disinformation:** While extreme, this may be your final data posted online.

Name Disinformation

Name disinformation will create an appearance that numerous people live at your residence. This could increase the delivery of mail and advertisements to your house. However, none of it will jeopardize your privacy. In fact, it will raise your level of privacy quickly.

Earlier, I explained how to use alias names in connection with your home address. When you activate internet service using a masked card, you have the option to use any name desired. The information you provide will eventually be released to third-party data companies. This is a form of disinformation. There are two routes you can take with this. You could choose a different alias name for every bill and service, which will generate chaos. This may be desired, but I prefer a more reserved approach. I choose a single generic name and place various bills under that name. This creates a strong appearance that this person is the true resident. Even if you place your utilities in the name of a trust or LLC, the companies will still want to attach a name to the account. Alias name consistency can create an appearance of legitimacy.

Next, identify a couple of popular magazines for which you are interested in a subscription. Conduct a search for that magazine plus “free subscription”. You may be surprised at the abundance of magazines that will give anyone a free subscription. I have found Wired, Forbes, and numerous technology magazines to continuously offer free trials. The most vital part of this exercise is that you do not provide anything close to your real name. Additionally, provide a different name for each subscription. I like to relate each name to the magazine that is being requested. The following could be a guide.

Men's Health: John Sporting
Money Magazine: Tim Cashman
Wired: Alex Techie
Food Magazine: James Cook

I also encourage you not to go overboard. Please only obtain subscriptions that you will read or pass on to someone who will enjoy them. There is no need to waste the product and immediately throw them in the trash. You will also eventually get frustrated if you have several issues arriving every week filling your mailbox.

Similar to magazines, I encourage you to identify a single newspaper that you would enjoy receiving. Newspaper subscriber databases are unique and cater to a specific market. This subscription information will leak out slowly to third-party companies. I do not recommend multiple newspaper subscriptions unless this is appropriate for your daily reading abilities. I enjoy reading the Wall Street Journal every day. A search online for “Wall Street Journal 39 week” will identify dozens of websites which will provide you a 39-week free trial of the paper. Complete the request and provide a unique name. I have found Mary S. Market to be

appropriate. You will begin receiving your print and digital editions within one week. At the time of this writing, I could not locate any completely free trials, but I did find a twelve-week subscription for \$12. You can cancel at the end without any further fees. If you choose this route, be sure to use a masked card which can block any future charges.

Trade magazines and mailings are designed to target a specific industry or trade. These are usually free by default and generate revenue from the advertising within the publication. Visiting freetrademagazines.com will display numerous options to consider. I encourage you to be cautious with this method. Many people will load up on magazines of interest and use a false name. While this is acceptable, it does create an association with your home address to your real interests. For example, if you subscribe to seven different web design magazines, and you are a web design artist, this could lead to an accurate profile about the people who live at your home. I would only choose this option if you do not take advantage of a magazine or newspaper subscription.

The time will come when you will need some professional work completed at your home. This will often happen the moment that you stop associating your real name with your home address. Use this as a disinformation opportunity. Consider the following example.

A friend recently discovered that he needed a new roof. Calling a stranger on Craigslist and paying cash would have been acceptable for privacy concerns. However, he understandably wanted to hire a professional company and possess a valid warranty on the new roof. He had recently conducted a complete cleaning of his personal information on the internet, and was concerned that this could jeopardize his privacy.

I recommended that he identify the company that he wished to hire and ask them to provide a quote. He gave them his real address for the roof job, but provided the name of a fake contracting company that was similar to the name of his invisible LLC. If your LLC was named Particle Ventures LLC, you could provide Ventures Contracting. This allowed him to keep his real name away from the process and attach yet another type of disinformation to the address. Upon completion of the work, my friend possessed a written warranty attached to the address and not to a person. This would suffice for replacement if problems with the roof appeared. If you do not possess an invisible LLC, you could use the name of your trust.

Remember, we are not using any of these methods to commit fraud. We are only protecting our privacy and will pay any accounts in full. For most work like this, paying either cash or with a check is acceptable. It is not likely that the name on the check will be attached to the data from the work, but it is possible.

Address Disinformation

This is the most vital type of disinformation if you are trying to disassociate your real name from your real address. The goal with these methods is to create an illusion that you currently live somewhere that you do not. This will make accurate name searches difficult. Before proceeding, you should have an idea of which addresses you will be providing.

This section will explain how to create at least three valid addresses that you can intentionally associate with your real name. The purpose is to show recent activity if someone was to search for you within a people search service. These services always display the most current information first. Therefore, you may want to complete as much of the removal process as possible that is discussed later before providing this disinformation. Additionally, you would only want to do this after you have stopped associating your real name with your real address.

It is very important not to use another individual's home address. While it may not be illegal, it is not ethical and not fair to the other person. If you are hiding from an abusive ex, you do not want to put someone else in danger when he or she decides to break into a house believing it is yours. If you are a police officer trying to protect your family from criminals seeking revenge, you should not send them to some stranger's house and let those residents deal with it. We will only choose locations that do not pose a threat to anyone.

The first address may be a place that does not exist. Many companies possess verification software that will identify invalid addresses. These programs can often be fooled by selecting addresses in new neighborhoods. The following instructions will easily identify a new address for you.

- Conduct a Google search for “new construction city, state”. Replace “city, state” with a location at least a few towns away from you. I also recommend clicking “Search Tools”, “Any Time”, and selecting “Past Year”. This will display recent results.
- Choose a search result that connects to a real estate website which displays new homes for sale. The newly planted grass, identical houses, and identical sale price in each listing are also indicators of a brand-new neighborhood.
- Conduct a search on Zillow.com for the highest number visible on the chosen street. You should see a house attached to this address. Increase the address by ten or twenty numbers. In this scenario, I searched 1017 Park Charles Blvd. Zillow informed me that there was no house at this address.
- Search this new address on Google maps and confirm the house does not exist. Switch to the satellite view and confirm there would not likely be enough land to add the number of houses necessary to create this address.
- Document this new address and use it for disinformation.

If this is too much effort, replicate a process which was previously explained in regard to fake apartment addresses. Locate a large apartment building; determine the highest unit number; and identify a higher unit number which does not exist. The apartment street address should pacify the verification systems, which often ignore specific unit numbers. I find this method to be the most accepted by address verification systems.

Occasionally, advanced verification software will identify a fake address as invalid. You may need to provide a real address that is listed as residential but does not belong to an individual family. You may want to choose the address of an emergency shelter. The residents in these are constantly changing, and most of them have 24-hour staff and security. Since many people must consider these a temporary residence, the addresses often defeat the most advanced verification services. Choosing a city and searching it online including the terms “shelter”, “men’s home”, “women’s home”, and “homeless” will usually provide options. I use this as a last option.

Public library addresses are almost always identified as commercial, but the addresses will pass standard validation. For most disinformation purposes, the address of any public building, including a library, will suffice. Now that you have some ideas for your new address, the next techniques will help you populate online records with this information.

A less invasive way of populating bad information about you on the internet is responding to television offers during infomercials. You have likely seen various offers for information about devices such as medical alerts, home security systems, and reverse mortgages on both daytime and late-night television. They all offer to send you an informational packet describing how they can help you in any situation. These are always a profitable business anticipating huge financial returns when they engage you for their services. Instead, I will use this as a way to mask my true home address.

I recently watched a commercial for a slow motorized device created to help the elderly and those with disabilities. It was a combination of a wheelchair and a moped that could move anyone around the street, grocery store, or mall. You are probably familiar with these “scooters”. I called the number and requested information. I used my real name and an address in a new subdivision that did not exist. I do not like to use real addresses because someone will need to deal with the junk mail that is received. This way, the mailings are simply returned to the business. I purposely provided a street name that I located called “Mobility Way”.

Within 90 days, while conducting a routine query of my name on people search websites, I located an entry for me on “Mobility Way”. I now know with certainty that this company shares personal information. If someone is trying to locate me, he or she will have one more address to research and be disappointed.

There is no need to wait in front of a television all night with the hopes of catching a great disinformation opportunity. The internet has thousands waiting for you at all times. Searching for any of the following topics will likely present numerous websites eager to send you a free information packet. Providing your new "fake" address will get you quickly listed within several marketing databases with this false information.

Home Scooter
Time Share
Home Alarm
Lawn Treatment Service
Home Food Delivery
Diabetes Supplies
Medical Alert Systems
Franklin Mint
Senior Citizen Vacation Tours
AARP
Cruise Lines

Please do not ever provide any real information about yourself, besides your name, to any of these services. Never provide a credit card number or any other type of payment information, as these types of companies are notorious for unauthorized charges. You should only use this technique to create the illusion that you live somewhere other than your real home. Additionally, if you have a common name, such as John Smith, address disinformation is not likely necessary and should be avoided.

Be aware that paper mailings will likely be delivered from, and returned to, the businesses that you contact. This is very wasteful for both the business and the planet. I encourage you to only perform the actions necessary to obtain your address disinformation goal. I do not encourage you to unnecessarily contact hundreds of companies. It only takes a few large companies to make an impact on your overall address identity.

Once you are in these marketing databases, you might consider updating your contact information. Assume that various people search websites now display the address information provided to these companies. This alone is a success, but we could take it to another level. Contact each of these companies and ask to update your address because you have recently moved. Provide a new random empty lot or apartment address. Eventually, you may see updated details appear on the people search websites. This can make accurate details harder to find or questionable as legitimate. I understand that this may be overkill for most, if not all, readers. I only present the ideas which enter my head, even if they are extreme.

Advanced Address Disinformation

The previous methods will provide a small layer of privacy disinformation. None of those tactics will fool the big players. Ordering marketing materials in your name to a non-existent address will not populate the desired information within premium data mining companies such as CLEAR, Lexis-Nexis, and TLO. These providers only purchase and distribute vetted data, and place emphasis on lines of credit and public records. Some people may want to push bad data to these services, but I urge caution before considering the following techniques.

In 2019, a client insisted on populating address disinformation into the premium data broker providers. He knew that a potential employer would be conducting a background check which included an inquiry into a premium data service. This client lived in an anonymous home with no ties to his true name. He would not consider providing his actual home address to the potential non-government employer. However, this company demanded to possess a “home address” for all employees. Any address provided would be matched to online records from the premium services. He needed an address to provide on the application which would be present within his premium records profile.

This approaches a grey area in terms of legalities. Lying to a private company about your home address is likely not a crime. Creating disinformation about your home address within data mining companies is also likely legal. Generating false data with the intention of fooling a background check enters new territory for me. If he were applying for a government position, I would have backed away from this request as it could easily cross the line of criminal behavior. Since this was a private organization, I decided to pursue the opportunity.

The first step was to choose an address. This was much more important than using Zillow to find a vacant lot. This needed to be precise, and a place where the world could assume that he lived there indefinitely. We chose a large apartment building near the place of potential employment. For purposes of this example, the address was 1212 State Street. Over 100 apartments were in the building. A quick physical sweep indicated that the apartment numbers followed a pattern of the floor number followed by the room number. The last apartment on the fifth floor was 528. The address for that apartment was 1212 State Street, Apt 528. There were no rooms with 30 in the address on any floor. Therefore, we chose an address of 1212 State Street, Apt 430.

Most address verification systems only consider the street address when associated with apartment buildings. Any apartment number should pass automated scrutiny as long as the street address is correct. My client was confident that the background checks did not include an interview of neighbors or physical inspection of the provided home address. He simply needed an online background check to confirm an address.

Next, we entered an AT&T cellular telephone store and ordered new service. This required a government ID, SSN, and soft-pull on his credit. This violates everything I teach for most clients, but this situation was unique. My client wanted new credit established in order to manipulate the details present in data mining databases. He picked the most inexpensive plan and lowest quality mobile device offered. He would not be using it, and would only abuse the credit inquiry to his benefit. He displayed his DL and provided his real DOB and SSN. He entered the new apartment address on the application and advised that he has recently moved into this new address. The AT&T employee ran the credit check and my client was approved. The system did not care about the mismatch of an address since the applicant was present in-store with a copy of valid identification. Replicating this attempt online would have likely failed.

I chose AT&T intentionally. In my experience, they always require a soft pull for any new line of service. They also provide the full application details, including the home address, to the services which they use for the credit pull. I have found AT&T to release more details to data mining companies faster than other providers. Also, AT&T provides a money-back guarantee. If my client were to return this unused phone within a few days, he is very likely to receive an entire refund. In this scenario, he wanted to keep the number for additional disinformation. The phone would stay in a Faraday bag at all times.

Next, he traveled to a local BestBuy and applied for an in-store credit card. Again, this made me cringe a bit, but I understood his intent. He provided his DL, DOB, SSN, and new apartment alias address. Since he was in-store with proof of ID, he was approved for a card with a low credit limit. He made a small purchase with this new line of credit and paid it off immediately before interest could accrue.

Within three weeks, we saw evidence of this new address on both his credit report and premium data report. While any investigator would see right through this, it was enough to pass the scrutiny of a standard background check using premium records. He then applied for, and received, his desired job.

For the record, I do NOT recommend these actions for the vast majority of my clients. It is usually unnecessary and can present additional problems. Any future background checks may need to explain this discrepancy on a public report. A government clearance may be denied when you disclose your antics of attempted disinformation with an alias address. There are many more reasons NOT to apply this technique than valid scenarios. I present this only as a tactic to possess in your arsenal of tools.

Proactive Online Content

I usually do not promote the creation of personal social network profiles. However, they can be very useful in some cases. I once consulted a young woman who was the victim of severe harassment by a man who was a former high school classmate of hers. His unwelcome approaches caused her to move and purchase a different vehicle. She was doing well at staying off his radar, but still knew he was looking for her. She created a Facebook page, added a couple of photos of her pet, and publicly displayed her location as a town over an hour away. While monitoring the Twitter account of her stalker, she observed him “check into” a bar in that very town, likely looking for her. While this does not solve the issue long-term, it provided enough uncertainty to confuse the stalker and waste his time.

Creating several social network profiles and including publicly visible location data can be beneficial. You can either make them very confusing by placing different locations on each profile, or place the same city on all of them to create a convincing situation. For most clients, I find LinkedIn to offer a great platform for disinformation. I can create an account, provide a real name, and choose any current workplace and location desired. This can quickly throw an adversary off my client’s trail if he is actively trying to locate him or her.

Aside from LinkedIn, I find Instagram, Twitter, and Facebook accounts valuable for online disinformation. However, always apply the digital security principles discussed earlier. After the accounts are created, never log in to them unnecessarily and always use a VPN. Never provide any sensitive details and never access the profile from your mobile device(s).

We can also rely on free services such as Carrd (carrd.co) to easily create a landing page on their servers. These will be indexed quickly and provide a realistic false internet presence. They appear more like a personal web page than a blog. While free WordPress pages can replicate the details for this purpose, I find them to appear suspicious. A page from Carrd appears much more professional and realistic. I prefer single pages within the “Profile” section. I created a demo page at <https://michaelbazzell.carrd.co> in less than five minutes. By connecting my disinformation social networks to this landing page, I encourage search engines and data collection companies to associate the data, such as the fake address, with the dossier they store about me. Eventually, this inaccurate data will be populated across the internet. When I see “UNIT PH51” appear within public databases, I will know that the information was scraped from this page.

If you create appropriate online content about yourself and promote it within search engines, it becomes more relevant to Google in terms of search results. The longer you “age” these pages, the more weight they hold when someone searches your name. The goal is to provide enough “good” online content so that the “bad” stuff is more difficult to find. I have found the following to provide the most impact toward an online search in your name.

You could also consider free blogs on WordPress, Weebly, Wix, and other sites. Your blog should include your name and possibly vague or inaccurate location data. Consider a test example of michaelllezzab.wordpress.com. I created this page for free under the name of Michael Llezzab. If you search that full name, or a fictitious email address which I created of q9u7uaxbspas@opayq.com in Google, you should be linked to the blog(s). If a new website pops up with defamatory content about that name, it will likely appear beneath the results of my aged blog. The more activity within the blog, the higher the preference by search engines.

Websites such as ifttt.com can be configured to automatically populate content to your blog every day. You can see that my example blog receives updates automatically without any need to log in to it. This tells Google that the site is active and places priority over dormant sites. The following instructions will populate your current free WordPress blog with every new post created by another blog hosted at krebsonsecurity.com. This will result in a site similar to mine with constant new content, all automated behind the scenes.

- Create a free WordPress blog at wordpress.com. Supply your real name and any inaccurate details desired, such as a false telephone number and burner email address. Remain logged in to this account in your browser.
- Create a free account with If This Then That at ifttt.com. Search for “WordPress RSS” in the top search field and select the “RSS to WordPress” option. Click the “On” switch and it will ask for your WordPress credentials. Since this is a free throw away blog, I do not object to sharing this unique password. Save and enter a new feed item of “krebsonsecurity.com/feed”. Save your entry.
- If you do not see the blog updates on the home page, make sure that “Your Latest Posts” is selected in the Settings > Customize > Homepage Setting menu.

Ideally, you will create numerous blogs which should force any undesired content to later pages in the search results. In my experience, it can take many months before Google indexes these pages. I have also posted numerous resumes which contain inaccurate details for my clients. I have found resumes to be constantly scanned and collected by recruiting services, and this quickly becomes populated online. In one scenario, I uploaded a resume in my client’s name with a false telephone number, email address, and city of residence. This was replicated across 14 websites. Today, when you search her name, the first two pages of results are nonsense that does not expose her or display any negative statements. If someone decides to create a negative site about her, it will be buried within these deliberate results. The goal is to populate enough neutral content about yourself in order to suppress any potential negative postings. A good investigator will always dig through every search result. However, the casual internet searcher may not make it past the first page. If you want to generate more traffic to these profiles and an overall higher confidence that the information is legitimate, consider a simple personal landing page on a shared web host with a custom domain, as explained next.

Personal Website & SSL Certificates

Personal websites on your own domain can offer a stronger layer of disinformation. I purchase a domain for many clients associated with their real name, similar to michaelazzell.com. I then place a static website with inaccurate details, including location and contact information on a shared host. Search engines index these sites quickly and place them as a priority within search results. I have placed a live example online at yourcomputernerds.com. This page includes a royalty-free stock image, false contact details, and links to multiple social networks. These links help convince data mining websites that the information is real. The site was created using free templates from html5up.net. It appears professional and convincing.

I find Namecheap the most affordable option for this purpose, and the lowest tier of hosting (\$30 annually) is usually sufficient. Unfortunately, Namecheap makes it difficult to provide your own SSL certificates for your domain in order to sell you an annual option at an inflated rate. I always recommend an SSL certificate for every website. This is not only an appropriate layer of protection for your visitors, but it also helps elevate your search results on Google and Bing. The following steps are quite technical and should be approached cautiously. They are designed for Namecheap, but should work with most shared web hosts which provides access to a cPanel dashboard. This is an advanced technique only for those comfortable with cPanel and SSH who want to avoid annual SSL fees. Conduct the following within cPanel.

- SSH Access > Manage SSH Keys > Generate a new key > Generate Key
- SSH Access > Manage SSH Keys > Manage > Authorize
- Manage Shell > Enable SSH

Conduct the following within Terminal (Linux or Mac). Replace any uppercase text.

- ssh CPANELUSERNAME@CPANELSERVERADDRESS -p 21098
- curl https://get.acme.sh | sh
- source ~/.bashrc
- acme.sh --register-account --accountemail YOUR@EMAIL.COM
- crontab -l | grep acme.sh
- acme.sh --issue --webroot ~/WEBSITEFOLDER -d DOMAIN.com -d www.DOMAIN.com --staging
- acme.sh --issue --webroot ~/WEBSITEFOLDER -d DOMAIN.com -d www.DOMAIN.com --force
- acme.sh --deploy --deploy-hook cpanel_uapi --domain DOMAIN.COM

After completion, reverse the cPanel steps to delete the SSH keys and disable SSH access. You should now possess an SSL certificate for your site which will auto-renew every 90 days.

Telephone Disinformation

Receiving unwanted telephone calls from telemarketers can be annoying. Calls from them to random numbers are unavoidable. However, targeted calls specific to you can be extra frustrating. You have already learned how to eliminate public record of your telephone number. You may now want to populate disinformation to prevent a person or business from discovering your true home or cellular telephone number.

Before you can provide the false telephone number information with hopes of it being attached to your name within public databases, you must select some appropriate numbers. Most importantly, you never want to provide a false number that belongs to another individual. That is not only rude, but it can also jeopardize that person's right to privacy from unwanted callers. Instead, focus on telephone numbers that either do not exist or belong to services that are never answered by an individual.

My favorite telephone numbers for disinformation are numbers that are always busy and cannot be answered. These were once abundant, but many of them have now been assigned to customers. There are still two large groups of telephone numbers that will always be busy when dialed. The following sets of numbers should work well.

909-661-0001 through 909-661-0090
619-364-0003 through 619-364-0090

The 909 area code serves the Los Angeles area of California and the 619 area code serves the San Diego area. These were early line numbers when service began in these areas and the numbers should not be assigned to any customers. Since these are not toll-free numbers, they should not be flagged as non-residential. Because numbers are ported so often, possessing a number in another area code should not raise any suspicion. When you give someone a number that is always busy, it does not create the appearance of a fake number. These may appear real to a person that would otherwise question the validity of a given number.

There are plenty of unused numbers that announce "disconnected" when dialed. Most of these are temporary and will be assigned to a customer at some point. The following range of numbers all announce a "non-working number" when dialed. The area code serves Pennsylvania. Giving one of these numbers to a person or business can enforce a desire to not be contacted. Always test the numbers which you choose before using them.

717-980-0000 through 717-980-9999

One of the quickest ways to associate a false telephone number with your real name is to enter various contests. You have probably seen a brand-new vehicle parked inside your local shopping mall. A box next to it likely contained blank pieces of paper asking for your name, address, and telephone number with promises that someone would win the vehicle. Have you ever known anyone that won a vehicle this way? I do not.

Instead, these gimmicks are often used to obtain a great list of potential customers that might be interested in automobiles. In one example, shopping malls across the country held a contest to win a car. A shiny Mustang was parked next to the entry box. However, they did not disclose that only one winner for the entire country would be announced. Furthermore, that winner did not get a new car. Instead, they were offered a small check to cover a used car purchase. Sneaky. The content obtained from the entry forms is often combined with other contest data and sold to numerous companies. Eventually, the provided information is attached to you through a marketing profile that may follow you forever.

In years past, I have always laughed at the idea of entering these contests. Today, I never pass up this opportunity. I always provide my real name, my false address from the address disinformation section mentioned earlier, and one of the “busy” telephone numbers previously listed. I like to use different numbers every time and watch for any online associations to me from these numbers. I then know which contest companies are selling my information.

Most grocery stores have a shopper’s card program which provides discounts on merchandise. These are portrayed as opportunities to save money for being a loyal customer to the brand. In reality, these cards are closely monitored to learn about your shopping habits. This data is used to create custom advertising and offers. The only benefit of joining this program is the savings on the items which you purchase. The risk of joining is the guaranteed profile that will be created about you and sold to interested parties. However, you can enjoy the benefits without jeopardizing your privacy. This is a great opportunity for telephone disinformation.

Practically all of the stores which utilize this type of savings program allow you to access your account by the telephone number that you provided during registration. You are not required to provide or scan your shopper’s card. You can simply enter your telephone number to obtain the savings and attach your purchases to your profile. I have found the telephone number of 867-5309 to work at most stores.

This number may not look familiar, but say the number out loud. This was the title of a song by Tommy Tutone in 1982 that gained a lot of popularity. This number is currently assigned to customers in most area codes. In fact, it is often sought after by businesses due to the familiarity. I never use this number with services that may try to contact me. Instead, I only use it when I register a shopping card at a grocery store.

If I am shopping in Chicago, I use an appropriate area code, such as 847. If you ever find yourself at a Safeway store anywhere in the world, you can use 847-867-5309 as your shopper's card number and it will be accepted without hesitation. If you find that this number does not work at another chain, you should consider requesting a shopper's card and provide it as your number.

When I created this account, I provided my real name, the disinformation address discussed earlier (which does not exist), a Chicago area code, the 867-5309 number, and a specific email address from an email forwarding service. I will never use that email account again, and will know which company provided my information when I receive unwanted email at it. I can now provide 847-867-5309 as my member number when I shop at Safeway in order to benefit from the advertised sale prices. Now, you can too.

As a community service, I create new accounts at every store that I can using the number of 847-867-5309. The more strangers that use this number during their shopping, the more anonymous we all are. The data collected by the store will not be about one individual. Instead, it will be a collective of numerous families. If you locate a store without a membership with this number, please consider activating your own card with address disinformation. Within weeks, this information will be associated with your real name. It will add an additional layer of anonymity by making any present information difficult to find and harder to prove accurate.

In 2021, I began seeing intentional blocking of any grocery rewards account containing a telephone number which includes 867-5309. It seems they have caught on to us. Because of this, I have begun a new telephone disinformation campaign with the number 248-434-5508. This is a VOIP number which plays an excerpt of Rick Astley's 1987 hit "Never Gonna Give You Up" in the outgoing message, which is also known as a Rick Roll.

I provide this number to grocery rewards systems whenever I can. If you do the same, we can create global coverage and all benefit from the usage. Anytime you find a business which requires member discount cards, and the number does not work, please apply for membership with this number and the name of Rick Astley. Together, we can escape the abuses of these systems.

I suspect others are now aware of this number, as it is listed as a verified number registered to "Rick Astley". The web page at <https://www.callercenter.com/248-434-5508.html> is one of dozens of sites which announce this association. This is an example of a successful telephone disinformation campaign.

Business and 411 Disinformation

Regardless of whether you desire name, address, or telephone disinformation, you should consider business listings. Most of these types of websites allow a personal name to be used instead of a business name. Any data provided will replicate all over the internet quickly. The first service which I submit is listyourself.net, followed by Google Maps and Yelp.

The irony of suggesting these free services is that most of my clients want to avoid them or remove their information. Any data provided here, such as your name and address, will be populated across multiple people search websites within weeks. However, we can use this as a strong disinformation strategy. Before conducting any of the following tasks, consider your goals and what types of disinformation you want to be publicly available. You cannot change your mind later on this one. Whatever you give them is permanently public data. Consider the following steps I took on behalf of a client.

This client had successfully moved into an anonymous home, but knew her abusive ex-boyfriend had been released from jail and was actively pursuing her new location. A disinformation campaign was appropriate in her scenario. I visited listyourself.net and chose “Individual, personal or business listings”. I then provided the following details for each field.

- Phone number: I chose a telephone number of the hotel where I was staying at the time, in a city far from the client’s home.
- Name: I provided my client’s real name.
- Country: I entered my client’s true country.
- Address: I supplied an address of a large apartment building in a city far from the client’s home. New York City has many buildings with over 500 units each. This is the address I will publicly associate with my client, without an apartment number.
- Email: A ProtonMail alias address used for “junk” in the name of the client. This address is not associated with any online accounts or login portals.
- Validation Method: I chose the “Call me with a spoken code” option.

This service will waive any fees as long as they can confirm you have provided a true telephone number. Before I clicked “Add Listing”, I took my laptop to the front desk of the hotel and spoke to the front desk clerk. I told her I was trying to connect to a web call with my boss, but it wants to verify my location. I asked “Can I have them call your main line and have them give me a code?”, which she happily allowed. If met with resistance, you could show your “cracked screen” decoy phone which was previously explained. The telephone rang, she answered, and repeated the automated code she was given during the call. My listing was approved. Next, I navigated to www.google.com/business and signed in with an alias Google account which I only use for this purpose. I then conducted the following steps.

- Enter the name of my client as the business name.
- Confirm I wish to add a location.
- Enter the address used previously, and click “Next”.
- Confirm that customers are not served outside this location.
- Provide a generic category such as “Personal Trainer”.
- Leave the contact details blank.
- Click “Finish”.
- Choose the options to “Verify by Phone”.
- Provide the same hotel number.
- Repeat the process with the front desk, entering the code provided.

Some people have reported that they do not receive the option to verify by phone, and can only verify with a mailed postcard. I suspect this is due to the Google account being used. My account may have been allowed because it has been active for many years and has activated numerous businesses. If you do not receive the option to verify by phone, do not request a postcard and move on.

Next, I navigated to biz.yelp.com/signup_business/new/ and registered my client for her own personal Yelp page. I provided the same real name, alias apartment building address in the city used previously, junk email address, and a Google Voice number reserved for disinformation purposes. I was immediately sent an email to verify the account, and was forwarded to a page to create a Yelp account for the client. I completed the registration and was asked to verify the telephone number via confirmation code. The Yelp account was then active.

Within a few days, searching my client’s name on Google revealed a Yelp page identifying her home trainer business being located in a large apartment building in New York. Google Maps eventually confirmed this address for her home-based business. Her name, alias address, and number were populated on numerous 411-style websites within two weeks. That should keep the abusive ex-boyfriend busy for a while.

These services are constantly closing any loopholes which we use to exploit their services for our own benefit. By the time you read this, you may discover that these specific examples no longer work due to abuse. If this happens, use the overall strategies and identify new ways to supply business disinformation. If you strike gold, consider sharing your tactic with me through my website.

Death Disinformation

I hesitate writing this. However, I once had a client who needed to “die” digitally. She had no immediate family, a few close friends, and a dedicated former lover trying to harm her at any chance he could find. During an initial consultation, she stated “I wish he thought I was dead”. I cautiously discussed the possibility, which she immediately demanded to be executed. The most bang-for-your-buck option is an obituary in the Legacy network of newspapers.

You can navigate to legacy.com > Obituaries > Submit an Obituary > Select a state > Select a newspaper. You will need to submit the obituary directly to the local paper of choice, and anything printed will be acquired by legacy.com and distributed. Expect a small fee. This will make an obituary extremely public, which can never be reversed. The obituary on legacy.com can be shared on social networks, and really “sells” the death.

Use caution, because some newspapers demand a death certificate. I have found extremely small newspapers near the town of birth of the target are less likely to demand this versus large city newspapers. For extra credit, consider submitting a memorial and photo to Find A Grave at findagrave.com. If your Photoshop skills are not sufficient, contact an online tombstone maker and ask for an example of how your deceased relative’s details would look (providing your information). They will create a realistic image and submit it to you for approval.

Overall, I never recommend this strategy. If you are in a situation regarding this extreme activity, contact me first. This could have a severe impact on future credit, employment, relationships, and sanity. If you conduct any level of research into faking your own death, you will mostly find stories of people who were caught doing this. For more information, read *Playing Dead* by Elizabeth Greenwood. I never encourage anyone to commit full pseudocide (faking your own death). Traditionally, this is done to collect life insurance funds, evade outstanding arrest warrants, get out of paying various loans, or simply start over with a new identity. Unless you plan on living in the mountains without any source of income, it simply will not work. Although no federal or state statutes explicitly ban pseudocide, you are likely to commit crimes such as conspiracy or fraud during the process.

My colleague “Mike A.” offers one last piece of advice. If you receive undesired mail, such as advertisements, in your real name at your home, and you have asked to be removed from the mailing list, consider a death announcement. He purchased a rubber stamp from a local office supply store which prints “Return to Sender - Addressee Deceased” in red ink on any unsolicited mail he receives in his name. He then drops the envelopes in a nearby mailbox for return to the sender. This seems to have a better outcome than a polite request to be removed. I am ashamed I did not think of this. Please note this will likely only work with first class mail, as the post office does not return flyers and other bulk mail.

Disinformation Examples & Results

In 2021, I launched my own disinformation campaign as a test to see how quickly I could populate inaccurate details. I first identified an address in Los Angeles which possessed thirty-five luxury apartments. Each address possessed an amendment of PH and a number, such as PH1 and PH9, to represent Penthouses number 1 through 35. I decided to only use PH40 and above in order to prevent any attacks against anyone residing in the building.

My first address used was 105 S Doheny Dr, PH41, Los Angeles, CA 90048. I used this to register a domain and intentionally declined the domain registration protection service. Almost immediately, I began receiving spam email messages and offers for web design. Within 30 days, my true name and fictitious address was present within a “Leads” dataset sold to mobile app design businesses. Today, this exact address is associated with my name on two public websites. The Whois data for this domain, which announces my false details, can be viewed at <https://who.is/whois/yourcomputernerds.com>.

I created a disinformation landing page at <https://yourcomputernerds.com/> with PH42 as my unit number. The image of “me” is a license-free photo from unsplash.com which can be uploaded to any site desired without attribution. I used the Rick Roll telephone number previously explained and provided an email address of mb@yourcomputernerds.com. I associated Twitter, Facebook, and LinkedIn profiles. This page has been indexed by every major search engine and has been scraped by dozens of people search websites. I see this address offered on one popular “Background Check” service when my name is searched.

Next, I created a Twitter account at <https://twitter.com/MichaelBazzell0>. It displays my home address as PH43 and includes a false date of birth and link to the domain I associated with the previous address. This generates a link between these two resources and starts to convince the online artificial intelligence machines that I am real.

My Facebook profile is at <https://facebook.com/100010658471564>. It also contains the same photo, a link to my Twitter page, my disinformation website, and vague location details. This continues the population of data to confuse the machines. I provided an address of PH44, but I have yet to see this data surface online.

My LinkedIn profile is located at <https://www.linkedin.com/in/michael-bazzell-a83572122/>. It contains the same image in order to continue the connection to previous content. I provided PH45 as my apartment number and supplied false alumni and employer details. Approximately 60 days after account creation, I observed this unique address associated with my name inside a recruiter’s database, which was obviously scraped from LinkedIn.

I submitted my address unit as PH46 at listyourself.net, but it has yet to surface online.

Disinformation Concerns

Several government employees have expressed concern to me about the risks of removing all personal information from the internet. Their thinking is that if there is no information about you it could be a red flag that you are affiliated with the intelligence and/or special operations communities and could cause you to come under suspicion in a foreign country. This creates quite a conundrum.

If members leave all their personal information on the internet, their spouses and children could be exposed and placed in danger. This is becoming even more important as we are starting to see targeted terrorism and doxing of military personnel within the borders of the United States. Alternatively, doing so may compromise their status by giving them a digitally “different” profile. I agree entirely with this logic. However, I disagree with the suggestions I have heard for solving this problem. Most of these suggestions are to essentially do nothing and take a more passive posture on social media. This is not my approach.

My solution is to remove all real information to the maximum extent. I believe you should make your home, your vehicles, your children, and your spouse as difficult to identify as possible. Only then will you be able to sleep soundly at night, secure in the knowledge that you and your family are a very difficult target to locate. However, I do not believe you should stop there. My opinion is that disinformation in this case is as good as real information. If the person reviewing it is overseas and finds five separate records of your “home” online, the scrutiny will likely end there.

I am also not opposed to creating social media disinformation. A social media account that is in your true name, but contains no accurate information, will make you look real while preventing you from being compromised. I do not recommend you associate yourself with a social media account under a different name, especially if the account has photos of you. This will almost certainly have the effect of making you look even more suspicious. The more thorough your disinformation campaign is, the more protection it will afford you.

In some agencies or departments, you may be prohibited from doing this yourself. You should check your department, agency, or headquarters policy before undertaking this. Another concern that has been expressed to me is that if you need this level of protection the individual’s organization will “take care of it”. While this may be the case in some instances, I encourage you to take responsibility for your own security and safety where permissible.

Monitoring

Now that you possess an invisible home with disinformation attached to it, you should continuously monitor your progress. Searching for yourself and your family within various people search websites will confirm your success at staying invisible. This should be conducted monthly until you are confident that any new online data would be inaccurate. Your success at remaining invisible to the growing number of personal data collection organizations will be reliant on your constant monitoring for any new leaks of your details on the internet. I would like to add one technique that I have found valuable for those desiring an aggressive approach toward monitoring situations where other people may be searching for details about them. **Canary Tokens** (canarytokens.org) offers an advanced way to monitor this behavior.

This free service allows you to create a Microsoft Word document, among other options, including PDF files, which includes a tracking script within. Anyone who opens the document will unknowingly launch the script which will collect the user's IP address, approximate location, operating system, and browser information. While an adversary could easily block this type of collection with a tracking script within a website or email, it is more difficult to stop within a document. Consider the following example.

I created a Canary Token document with a title of Michael Bazzell's Home Address and uploaded it to a public document storage site. When a person conducts a search for my name and sees this file, he or she is likely to open it, hoping to finally have my home details. The document is blank, but I am immediately sent the following information.

Date: 2019 Mar 15 16:34:25

IP: 193.0.108.42

Country: US

City: Marietta

Region Georgia

Organization: Comcast Cable

Language: en-US

Platform: MacIntel

Version: 74.0.3729.131

OS: Macintosh

Browser: Chrome

You now have knowledge that someone may be searching for you. These details are the exact data obtained from someone opening the "bait" document. This information tells me that someone was likely researching me from Marietta, GA, on a Mac running Chrome. The IP address confirms they use Comcast as their ISP. I do not know their identity or exact address, but this reveals a potential threat.

In 2021, I began noticing less success with monitoring via online documents. Today, I use the "Web Bug / URL" token, which is less likely to block monitoring. This allows you to enter an email address and be provided a URL. Anyone who clicks the URL will share their details with you via an email message.

Doxing Attempts

Many of these methods may seem ridiculous and inappropriate. If no one ever tries to find you, none of this is necessary. Many of my clients are targeted often, and I like to have false trails leading to inaccurate data. I have also found this to be beneficial for myself. In October of 2018, I was on the receiving end of a full doxing attack.

Doxing is the attempt to search for and publish private or identifying information about a particular individual on the internet, typically with malicious intent. Someone had posted information about a group called 4Chan/8Chan on my online forum. This group is known for hateful posts, doxing, e-swatting, and other malicious activities. Word had spread to the 4Chan/8Chan community that my site was talking about them in a negative way. They decided to attack me as the owner of the site.

Multiple people scoured the internet for any personal information about me. They believed they were successful, but did not uncover anything valid. The cell number they located was a Google Voice account provided on a Facebook page which I have never used. The home address they located was a non-existent house in my former city of residence. The email addresses they found were all intentional burner accounts which did not reach my true inboxes. They were effective in their search, but the data was simply inaccurate. I never predicted a doxing attempt toward me, but I was glad I had taken the necessary precautions ahead of the attack. You can hear more about this incident on my podcast (Episode 096-Lessons Learned from My Latest Doxing Attack).

This seems like an appropriate time to remind readers that we never know when we will be a victim of an online attack. In 2017, two online gamers engaged in a feud over a \$1.50 bet. This resulted in a swatting attempt toward one of the players. Tyler Barriss called the Wichita police from his Los Angeles home falsely reporting a shooting and kidnapping at the Wichita address of the other gamer. Police surrounded the home and Andrew Finch emerged from the front door confused about the commotion. After raising his hands at the order of police, he lowered one hand toward his waist. An officer shot him, killing him immediately. Tyler Barriss had conducted dozens of similar calls prior to this in order to harass other online gamers. This incident resulted in a 20-year prison sentence.

It does not take much today to upset someone to the point of taking malicious action against you. The internet has made it easier than ever to locate someone's home address within seconds. Being proactive by creating a safe and anonymous home is the first step toward preventing online attacks. Disinformation provides another strong layer of protection.

Contact Information Abuse

Everywhere we turn, there are attempts to collect our data. Companies want your phone number and email address in order to bombard you with marketing. The data collected becomes stored in company databases which are later sold, traded, leaked, or breached. The aftermath becomes our problem. Because of this, I am cautious to ever use personal communication accounts and rely heavily on forwarding services which were explained earlier. However, there will always be unintentional exposure. Consider the following scenarios.

Appointment Check-in Systems: In 2019, I scheduled an appointment to see a chiropractor before a long business trip. I was notified that they rely on a digital check-in system which now requires me to provide a valid email address or cellular telephone number through a series of iPads on the counter. I had never provided any contact details to this service, so I was not sure what to provide. The staff was very helpful and instructed me to use my first name then @123.com. Apparently, many of these systems accept any email address which ends with @123.com. I recorded one interaction of this for an introduction to my podcast (episode 143). If I had provided a real email address or number, I suspect it would have been abused.

Lodging Requirements: In 2019, I checked into a resort where I was presenting a cyber keynote the following day. My room was prepaid by the conference and attached to the master bill. However, the clerk demanded I provide a valid cellular telephone number and email address. I respectfully declined and she informed me that she could not complete the check-in process without this information. I supplied a random number which was accepted. However, she stated that my email address would need to be verified via a response to a message before she could issue access to my room. She stated that the email address would only be used to contact me in the case of an emergency. I politely advised that I could be contacted at my room if there was an emergency. She did not budge. I provided a 33Mail account which was rejected by the system. Apparently masking services were blacklisted. I reluctantly provided a ProtonMail alias, which was accepted. I told her that I would be forwarding any spam to her if the contact details were abused, and collected her business card from the counter. Within 24 hours, I began to receive marketing emails from the resort. I quickly created a rule which forwarded any messages received from the resort to the clerk's email address. I suspect she was not amused.

This is a tactic which I have used often when a company will not remove me from a mailing list. If I start to receive unwanted and unauthorized spam from a business, I identify the email addresses of any executives. I then create an email rule which forwards to them all messages which I receive from that company, then immediately sends them to my trash. In my experience, my email address is quickly removed from their list once an executive complains about the emails coming from me.

Personal Data Removal

In the unfortunate scenario where you locate accurate personal information on a website, such as your name and home address, don't panic. I maintain a continuously-updated workbook of data removal (opt-out) options on my website at <https://inteltechniques.com/EP>. You will find updated digital versions of the entire workbook there and a static offline copy within the next several pages. These present hundreds of invasive websites and the options for requesting removal of exposed information. The removal process of your information is usually easy, with a few exceptions. Most services will offer you a website to request removal of your details. These direct links are often hidden within fine print or rarely visited pages. My goal in this workbook is to take the research out of the removal process and simply tell you where to start. Each removal summary will display several pieces of information about each service that I have identified. The following structure outlines the data which is displayed throughout this content.

Service: The name of the service and website

Removal Link: The direct link for online removal, if available

Contact: Any email addresses that will reach an employee responsible for removal

Notes: Any special instructions

All resources are listed in alphabetical order for easy reference. The data supplied in the email address field could be used for unsuccessful removal attempts. If the official removal process for that service does not meet your needs, I recommend sending an email to the company. I have tried to locate email addresses of employees that appear to be responsible for removal requests. I suggest the following message be sent from the anonymous email address that you created earlier.

I have been unsuccessful in removing my personal information from your website. Per the information provided from your privacy policy, please remove the following from your service.

Full Name (As appears on their service)

Physical Address (As appears on their service)

Telephone Number (ONLY if it appears on their service)

Email Address (ONLY if it appears on their service)

I have found the "Most bang for your buck" removals to be Spokeo, Radaris, Whitepages, Intelius, BeenVerified, Acxiom, Infotracer, LexisNexis, and TruePeopleSearch. Removal from these services will trickle down to many of the smaller sites mentioned on the following pages. I recommend that people start with these first, wait about one week, and then start to tackle the remaining sites. If a service asks for a photo ID or "selfie", just upload a random image generated at thispersondoesnotexist.com. They usually don't look at the picture because most verification is automated. If you want to see the typical details stored about you at the main data mining services, request your own LexisNexis data report at <https://consumer.risk.lexisnexis.com/request>. The following removal options were accurate as of May 2021. Updated content may be available on my website. These are mostly targeted toward U.S. people, but a few services apply internationally.

Service: 411 - <https://411.com>
Removal Link: None
Contact: support@whitepages.com
Notes: Remove entry from whitepages.com

Service: 411 Info - <https://411.info>
Removal Link: <https://411.info/manage/>
Contact: support@411.info, admin@411.info
Notes: Online removal tool will complete the process.

Service: Acxiom - <https://www.acxiom.com>
Removal Link: <https://isapps.acxiom.com/optout/optout.aspx>
Contact: consumeradvo@acxiom.com
Notes: Online removal tool will complete the process.

Service: Addresses - <https://addresses.com>
Removal Link: <https://www.intelius.com/opt-out>
Contact: support@addresses.com, admin@addresses.com
Notes: Online removal tool will complete the process.

Service: Address Search - <https://addresssearch.com>
Removal Link: <https://addresssearch.com/remove-info.php>
Contact: support@addresssearch.com
Notes: Online removal tool will complete the process.

Service: Advanced Background Checks - <https://advancedbackgroundchecks.com>
Removal Link: <https://www.advancedbackgroundchecks.com/removal>
Contact: Unknown
Notes: Online removal tool will complete the process.

Service: Advanced People Search - <https://www.advanced-people-search.com/>
Removal Link: <https://www.advanced-people-search.com/static/view/optout/>
Contact: <https://www.advanced-people-search.com/static/view/contact/>
Notes: Online removal tool will complete the process.

Service: All Area Codes - <https://www.allareacodes.com/>
Removal Link: https://www.allareacodes.com/remove_name.htm
Contact: https://www.allareacodes.com/contact_us.htm
Notes: Online removal tool will complete the process.

Service: All People - <https://allpeople.com/>
Removal Link: Embedded
Contact: webmaster@allpeople.com
Notes: Select profile and choose “Remove Listing”.

Service: Anywho - <https://anywho.com>
Removal Link: None
Contact: ypcsupport@yp.com, press@yp.com
Notes: Select profile and choose “Remove Listing”.

Service: Ancestry - <https://ancestry.com>
Removal Link: None
Contact: support@ancestry.com, customersolutions@ancestry.com
Notes: Send message to both email addresses requesting specific information removal.

Service: Archives - <https://archives.com>
Removal Link: archives.com/optout
Contact: privacy@archives.com
Notes: Online removal tool will complete the process.

Service: Background Alert - <https://www.backgroundalert.com>
Removal Link: <https://www.backgroundalert.com/optout/>
Contact: customerservice@backgroundalert.com
Notes: Online removal tool will complete the process.

Service: Background Check - <https://backgroundcheck.run/>
Removal Link: Within result
Contact: <https://backgroundcheck.run/pg/contact>
Notes: Online removal tool will complete the process. Lookup name and select "Control this profile".

Service: Been Verified - <https://www.beenverified.com>
Removal Link: <https://www.beenverified.com/faq/opt-out/>
Contact: privacy@beenverified.com
Notes: Online removal tool will complete the process.

Service: BlockShopper - <https://blockshopper.com>
Removal Link: None
Contact: scarlett@blockshopper.com
Notes: Send email with removal request.

Service: Buzzfile - <https://buzzfile.com>
Removal Link: <https://www.buzzfile.com/Company/Remove>
Contact: info@buzzfile.com
Notes: Online removal tool will complete the process.

Service: Caller Smart - <https://www.callersmart.com>
Removal Link: <https://www.callersmart.com/opt-out>
Contact: <https://www.callersmart.com/contact>
Notes: Email submission bypasses account creation requirement.

Service: Callyo - <https://callyo.com>
Removal Link: None
Contact: callyo.support@motorolasolutions.com
Notes: Email demanding removal of information associated with your number.

Service: Cars Owners - <https://carsowners.net>
Removal Link: None
Contact: <https://carsowners.net/feedback>
Notes: Email through the website requesting removal.

Service: Catalog Choice - <https://catalogchoice.org>
Removal Link: None
Contact: support@catalogchoice.org
Notes: Online removal tool will complete the process.

Service: Check People - <https://www.checkpeople.com>
Removal Link: <https://www.checkpeople.com/opt-out>
Contact: support@checkpeople.com
Notes: Online removal tool will complete the process.

Service: Check Them - <https://www.checkthem.com>
Removal Link: <https://www.checkthem.com/optout/>
Contact: support@checkthem.com
Notes: Online removal tool will complete the process.

Service: City-Data - <https://www.city-data.com>
Removal Link: <https://www.advameg.com>
Contact: others@city-data.com, legal@city-data.com
Notes: Go to www.advameg.com and submit an opt-out request.

Service: Clustr Maps - <https://clustrmaps.com/p/>
Removal Link: <https://clustrmaps.com/bl/opt-out>
Contact: <https://clustrmaps.com/bl/contacts>
Notes: Online removal tool will complete the process.

Service: Confidential Phone Lookup - <https://www.confidentialphonelookup.com>
Removal Link: Highlight entry and click “Do Not Display”
Contact: <https://www.confidentialphonelookup.com/contact/>
Notes: Online removal tool will complete the process.

Service: Contact Out - <https://contactout.com>
Removal Link: None
Contact: support@contactout.com
Notes: Send email with removal request.

Service: Core Logic - <https://www.corelogic.com>
Removal Link: None
Contact: privacy@ebureau.com
Notes: Online removal tool will complete the process.

Service: Cyber Background Checks - <https://www.cyberbackgroundchecks.com>
Removal Link: None
Contact: <https://www.cyberbackgroundchecks.com/contact>
Notes: Send email with removal request.

Service: DataChk - <https://www.datacheckinc.com>
Removal Link: None
Contact: <https://www.datacheckinc.com/contact.php>
Notes: Send email with removal request. Removes data from several subsidiaries.

Service: DirectMail - <https://directmail.com>
Removal Link: https://www.directmail.com/mail_preference/
Contact: donotmaillist@directmail.com
Notes: Online removal tool will complete the process.

Service: DMA Choice - <https://dmachoice.org>
Removal Link: <https://www.ims-dm.com/cgi/dncc.php>
Contact: ethics@the-dma.org
Notes: Follow instructions on removal link.

Service: DOB Search - <https://www.dobsearch.com>
Removal Link: Embedded into results
Contact: support@dobsearch.com
Notes: Search your name and click “Manage my listings” at bottom. Follow instructions.

Service: Email Finder - <https://emailfinder.com>
Removal Link: <https://www.beenverified.com/app/optout/search>
Contact: support@emailfinder.com
Notes: Online removal tool will complete the process.

Service: Epsilon-Main - <https://epsilon.com>
Removal Link: None
Contact: optout@epsilon.com, abacusoptout@epsilon.com, dataoptout1@epsilon.com
Notes: Send email with “Removal” as the subject to each address. Include name and address.

Service: Epsilon-Shopper - <https://epsilon.com>
Removal Link: None
Contact: contactus@shoppers-voice.com
Notes: Send email with “Removal” as the subject. Include name and address.

Service: Fama - <https://fama.io/>
Removal Link: None
Contact: privacy@fama.io
Notes: Send email with removal request.

Service: FamilySearch - <https://www.familysearch.org>
Removal Link: None
Contact: RochaJL@familysearch.org, [DataPrivacyOfficer@ldschurch.org](mailto>DataPrivacyOfficer@ldschurch.org)
Notes: Send email with removal request.

Service: Family Tree Now - <https://familytreenow.com>
Removal Link: <https://www.familytreenow.com/optout>
Contact: <https://www.familytreenow.com/contact>
Notes: Online removal tool will complete the process.

Service: Fast People Search - <https://fastpeoplesearch.com>
Removal Link: <https://www.fastpeoplesearch.com/removal>
Contact: <https://www.fastpeoplesearch.com/contact>
Notes: Online removal tool will complete the process.

Service: Fax VIN - <https://www.faxvin.com>
Removal Link: None
Contact: <https://www.faxvin.com/company/contact>
Notes: Email through website to request removal.

Service: Find People Search - <https://findpeoplesearch.com>
Removal Link: <https://findpeoplesearch.com/customerservice/>
Contact: support@findpeoplesearch.com
Notes: Online removal tool will complete the process.

Service: Free Background Checks - <https://freebackgroundcheck.us>
Removal Link: None
Contact: info@peepdb.com
Notes: Fax submission based on instruction listed on Privacy Policy page to 617-933-9946.

Service: Free Phone Tracer - <https://www.freephonetracer.com/>
Removal Link: <https://www.beenverified.com/app/optout/search>
Contact: privacy@freephonetracer.com
Notes: Online removal tool will complete the process.

Service: Free Public Profile - <https://www.freepublicprofile.com/>
Removal Link: <https://www.freepublicprofile.com/Removal>
Contact: <https://people.vidalud.com/Contact>
Notes: Online removal tool will complete the process.

Service: Full Name Directory - <https://www.fullnamedirectory.com>
Removal Link: <https://www.dobsearch.com/remove>
Contact: support@dobsearch.com
Notes: Online removal tool will complete the process.

Service: Glad I Know - <https://gladiknow.com/>
Removal Link: <https://gladiknow.com/opt-out>
Contact: support@gladiknow.com
Notes: Online removal tool will complete the process.

Service: GoLookup - <https://golookup.com/>
Removal Link: <https://golookup.com/support/optout>
Contact: support@golookup.com
Notes: Online removal tool will complete the process.

Service: Haines & Company - <https://www.haines.com>
Removal Link: None
Contact: criscros@haines.com, info@haines.com, custserv@haines.com
Notes: Send email with name and address and request to be removed from all databases.

Service: HPCC-USA - <https://www.hpcc-usa.org/>
Removal Link: <https://www.hpcc-usa.org/research/change-listing.html>
Contact: <https://www.hpcc-usa.org/research/contact-us.html>
Notes: Online removal tool will complete the process.

Service: ID True - <https://www.idtrue.com>
Removal Link: <https://www.idtrue.com/optout/>
Contact: support@idtrue.com
Notes: Online removal tool will complete the process.

Service: Infogroup - <https://infogroup.com>
Removal Link: None
Contact: contentfeedback@infogroup.com
Notes: Send email with "Opt-Out" as the subject. Include name and address.

Service: Infopay - <https://www.infopay.com/>
Removal Link: <https://www.infopay.com/optout>
Contact: <https://www.infopay.com/help.php>
Notes: Online removal tool will complete the process.

Service: Infotracer - <https://infotracer.com>
Removal Link: <https://infotracer.com/optout/>
Contact: <https://infotracer.com/help/>
Notes: Online removal tool will complete the process.

Service: Instant Check Mate - <https://instantcheckmate.com>
Removal Link: <https://instantcheckmate.com/optout>
Contact: privacy@instantcheckmate.com, support@instantcheckmate.com
Notes: Online removal tool will complete the process.

Service: InstantPeopleFinder - <https://www.instantpeoplefinder.com/>
Removal Link: <https://www.intelius.com/opt-out>
Contact: support@instantpeoplefinder.com
Notes: Online removal tool will complete the process.

Service: Intelius - intelius.com
Removal Link: <https://www.intelius.com/opt-out>
Contact: privacy@intelius.com
Notes: Online removal tool will complete the process.

Service: IntelligenceX - <https://intelx.io/>
Removal Link: None
Contact: <https://intelx.io/abuse>
Notes: Online contact option will complete the process.

Service: Kiwi Searches - <https://kiwisearches.com>
Removal Link: <https://kiwisearches.com/optout>
Contact: support@kiwisearches.com
Notes: Email request required.

Service: Lead Ferret - <https://leadferret.com>
Removal Link: None
Contact: removeme@leadferret.com
Notes: Email request required.

Service: LexisNexis/Accurint - <https://lexisnexis.com>
Removal Link: <https://optout.lexisnexis.com>
Contact: privacy.information.mgr@lexisnexis.com
Notes: Online removal tool will complete the process. You can upload digital documents.

Service: LexisNexis Direct Marketing - <https://www.lexisnexis.com>
Removal Link: www.lexisnexis.com/privacy/directmarketingopt-out.aspx
Contact: privacy.information.mgr@lexisnexis.com
Notes: Online removal tool will complete the process.

Service: LexisNexis - <https://lexisnexis.com>
Removal Link: <https://consumer.risk.lexisnexis.com/request>
Contact: privacy.information.mgr@lexisnexis.com
Notes: Follow instructions to request and remove info

Service: Locate Family - <https://www.locatefamily.com>
Removal Link: <https://www.locatefamily.com/removal.html>
Contact: <https://www.locatefamily.com/contact.html>
Notes: Online removal tool will complete the process.

Service: MashPanel - <https://www.mashpanel.com/>
Removal Link: <https://www.mashpanel.com/remove.php>
Contact: <https://www.mashpanel.com/contact-us>
Notes: Online removal tool will complete the process.

Service: Melissa Data - <https://melissadata.com>
Removal Link: None
Contact: paul.nelson@melissa.com or brett.mcwhorter@melissa.com
Notes: Send email with removal request.

Service: MyHeritage - <https://myheritage.com>
Removal Link: None
Contact: support@myheritage.com
Notes: Send email with removal request.

Service: MyLife - <https://www.mylife.com>
Removal Link: None
Contact: privacy@mylife.com
Notes: Send email with removal request.

Service: National Cellular Directory - <https://www.nationalcellardirectory.com/>
Removal Link: <https://www.nationalcellardirectory.com/optout/>
Contact: support@nationalcellardirectory.com
Notes: Online removal tool will complete the process.

Service: Neighbor Report - <https://neighbor.report>
Removal Link: <https://neighbor.report/remove>
Contact: support@gew3.org
Notes: Online removal tool will complete the process.

Service: Number 2 Name - <https://www.number2name.com>
Removal Link: https://members.infotracer.com/tspec/shared/assets/data_opt_out_form.pdf
Contact: None
Notes: Complete Infotracer Opt-out.

Service: Numberville - <https://numberville.com>
Removal Link: <https://numberville.com/opt-out.html>
Contact: <https://numberville.com/contact.html>
Notes: Online removal tool will complete the process.

Service: Nuwber - <https://www.nuwber.com>
Removal Link: <https://nuwber.com/removal/link>
Contact: support@nuwber.com
Notes: Online removal tool will complete the process.

Service: OK Caller - <https://www.okcaller.com/>
Removal Link: Embedded into pages
Contact: support@OkCaller.com
Notes: Within results, click "This is my number" then "Opt-out - Unlist".

Service: Old Friends - <https://old-friends.co/>
Removal Link: <https://old-friends.co/>
Contact: support@old-friends.co
Notes: Online removal tool will complete the process.

Service: Old Phone Book - <https://www.oldphonebook.com/>
Removal Link: None
Contact: paulmfield@gmail.com - lookupuk@gmail.com
Notes: Send request via email.

Service: Open Corporates - <https://opencorporates.com>
Removal Link: None
Contact: data.protection@opencorporates.com
Notes: Send removal request with public details via email.

Service: PCCare99 - <https://pccare99.com>
Removal Link: None
Contact: panchamithracreators@gmail.com
Notes: Send email with removal request.

Service: PeekYou - <https://peekyou.com>
Removal Link: www.peekyou.com/about/contact/optout/
Contact: support@peekyou.com
Notes: Online removal tool will complete the process.

Service: Peep Lookup - <https://www.peeplookup.com>
Removal Link: https://www.peeplookup.com/opt_out
Contact: hello@peeplookup.com
Notes: Online removal tool will complete the process.

Service: People By Name - <https://www.peoplebyname.com>
Removal Link: <https://www.peoplebyname.com/remove.php>
Contact: support@peoplebyname.com
Notes: Online removal tool will complete the process.

Service: People By Phone - <https://www.peoplebyphone.com>
Removal Link: <https://www.peoplebyphone.com/removal/>
Contact: support@peoplebyphone.com
Notes: Online removal tool will complete the process.

Service: People Data Labs - <https://www.peopledatalabs.com/>
Removal Link: <https://www.peopledatalabs.com/opt-out-form>
Contact: privacy@peopledatalabs.com/
Notes: Online removal tool will complete the process.

Service: People Finder - <https://peoplefinder.com>
Removal Link: <https://peoplefinder.com/optout.php>
Contact: support@peoplefinder.com, info@peoplefinder.com
Notes: Online removal tool will complete the process.

Service: People Looker - <https://peoplelooker.com>
Removal Link: <https://www.peoplelooker.com/f/optout/search>
Contact: west.privacypolicy@thomson.com
Notes: Online removal tool will complete the process.

Service: People Lookup - <https://peoplelookup.com>
Removal Link: None
Contact: support@peoplelookup.com, info@peoplelookup.com
Notes: Send your custom opt-out request form via fax to 425-974-6194

Service: People-Search - <https://www.people-search.org>
Removal Link: (Embedded in results)
Contact: info@people-search.org
Notes: Online removal tool will complete the process.

Service: People Search Expert - <https://www.peoplesearchexpert.com>
Removal Link: (Appears on result page)
Contact: support@peoplesearchexpert.com, info@peoplesearchexpert.com
Notes: Online removal tool will complete the process.

Service: People Search Now - <https://peoplesearchnow.com>
Removal Link: <https://www.peoplesearchnow.com/opt-out>
Contact: support@peoplesearchnow.com, info@peoplesearchnow.com
Notes: Complete form and mail to listed address.

Service: People Search Site - <https://www.peoplesearchsite.com/>
Removal Link: Embedded in profile
Contact: info@peoplesearchsite.com
Notes: Click the opt-out link (bottom right of profile), and follow instructions.

Service: People Smart - <https://peoplesmart.com>
Removal Link: <https://www.peoplesmart.com/optout-go>
Contact: privacy@peoplesmart.com
Notes: Online removal tool will complete the process.

Service: People Trace UK - <https://www.peopletraceuk.com>
Removal Link: https://www.peopletraceuk.com/Record_Removal_Request.asp
Contact: support@peopletraceuk.com
Notes: Online removal tool will complete the process.

Service: People's Check - <https://www.peoplescheck.com>
Removal Link: <https://www.peoplescheck.com/optout/index>
Contact: support@peoplescheck.com
Notes: Online removal tool will complete the process.

Service: People Whiz - <https://www.peoplewhiz.com>
Removal Link: <https://www.peoplewhiz.com/remove-my-info>
Contact: info@PeopleWhiz.com
Notes: Online removal tool plus email confirmation will complete the process.

Service: Persopo - <https://www.persopo.com>
Removal Link: None
Contact: support@persopo.com
Notes: Send email with removal request. Removes data from several subsidiaries.

Service: Phone Detective - <https://www.phonedetective.com/>
Removal Link: <https://www.beenverified.com/app/optout/search>
Contact: privacy@phonedetective.com
Notes: Online removal tool will complete the process.

Service: Phone Number Data - <https://www.phonenumberdata.net/>
Removal Link: None
Contact: phonenumberdata@live.com
Notes: Send email with removal request.

Service: Phone Owner - <https://phoneowner.com>
Removal Link: None
Contact: customer-service@phoneowner.com
Notes: Send email with removal request. Removes data from several subsidiaries.

Service: Phonebook (BT) - <https://www.thephonebook.bt.com/person/>
Removal Link: <https://www.bt.com/consumer/edw/privacypolicy/copyform/bt/#/>
Contact: support@productsandservices.bt.com
Notes: Online removal tool will complete the process.

Service: Pipl - <https://pipl.com>
Removal Link: <https://pipl.com/personal-information-removal-request>
Contact: support@pipl.com, mail@pipl.com
Notes: Online removal tool will complete the process.

Service: Plaid - <https://plaid.com>
Removal Link: <https://plaid.com/legal/data-protection-request-form/>
Contact: privacy@plaid.com
Notes: Online removal tool will complete the process.

Service: Property Shark - <https://www.propertyshark.com/>
Removal Link: None
Contact: support@propertyshark.com
Notes: Send email with removal request.

Service: Private Eye - <https://www.privateeye.com/>
Removal Link: <https://www.privateeye.com/static/view/contact/>
Contact: support@peoplefinders.com
Notes: Send email with removal request.

Service: Public Data Digger - <https://publicdatadigger.com/>
Removal Link: <https://publicdatadigger.com/removeprofile>
Contact: support@publicdatadigger.com
Notes: Online removal tool will complete the process.

Service: Public Data USA - <https://publicdatausa.com>
Removal Link: <https://publicdatausa.com/optout.php>
Contact: <https://publicdatausa.com/contact.php>
Notes: Online removal tool will complete the process.

Service: Public Info Services - <https://www.publicinfoservices.com/>
Removal Link: None
Contact: support@publicinfoservices.com
Notes: Send email with removal request.

Service: Public Mail Records - <https://publicemailrecords.com>
Removal Link: None
Contact: publicemailrecords@gmail.com
Notes: Send email with removal request. Removes data from several subsidiaries.

Service: Public Records - <https://publicrecords.directory>
Removal Link: <https://publicrecords.directory/contact.php>
Contact: support@publicrecords.directory
Notes: Send email with removal request. Removes data from several subsidiaries.

Service: Public Records Now - <https://www.publicrecordsnow.com/>
Removal Link: <https://www.publicrecordsnow.com/static/view/optout/>
Contact: <https://www.publicrecordsnow.com/static/view/contact/>
Notes: Online removal tool will complete the process.

Service: Public Records 360 - <https://publicrecords360.com>
Removal Link: <https://publicrecords360.com/optout.html>
Contact: optout@publicrecords360.com, privacy@publicrecords360.com
Notes: Complete opt-out form and email with ID to optout@publicrecords360.com.

Service: Public Seek - <https://publicseek.com/>
Removal Link: None
Contact: privacy@publicseek.com & support@publicseek.com
Notes: Send email with removal request.

Service: Publishers Clearing House - <https://pch.com>
Removal Link: None
Contact: privacychoices@pchmail.com
Notes: Send email with name and address and request to be removed from all databases.

Service: Radaris - <https://radaris.com>
Removal Link: <https://radaris.com/control/privacy>
Contact: support@radaris.com, info@radaris.com
Notes: Select your profile and submit to removal URL.

Service: Rehold - <https://rehold.com>
Removal Link: Embedded into pages
Contact: customer-support@rehold.com & <https://rehold.com/page/contact>
Notes: Click "Information Control" on right side of page and follow directions.

Service: Reveal Name - <https://www.revealname.com>
Removal Link: https://www.revealname.com/opt_out
Contact: support@revealname.com
Notes: Online removal tool will complete the process.

Service: Reverse Phone Lookup - <https://www.reversephonelookup.com>
Removal Link: [reversephonelookup.com/remove.php](https://www.reversephonelookup.com/remove.php)
Contact: support@reversephonelookup.com, info@reversephonelookup.com
Notes: Online removal tool will complete the process.

Service: Sales Spider - <https://salespider.com>
Removal Link: None
Contact: support@salspider.com
Notes: Locate profile and select "Delete this profile".

Service: Search Bug - <https://www.searchbug.com/>
Removal Link: <https://www.searchbug.com/peoplefinder/how-to-remove.aspx>
Contact: support@searchbug.com
Notes: Follow online instructions at <https://www.searchbug.com/peoplefinder/how-to-remove.aspx>

Service: Search People Free - <https://www.searchpeoplefree.com>
Removal Link: <https://www.searchpeoplefree.com/opt-out>
Contact: <https://www.searchpeoplefree.com/contact-us>
Notes: Online removal tool will complete the process.

Service: Smart Background Checks - <https://www.smartbackgroundchecks.com>
Removal Link: <https://www.smartbackgroundchecks.com/optout>
Contact: <https://www.smartbackgroundchecks.com/contact>
Notes: Online removal tool will complete the process.

Service: Social Catfish - <https://socialcatfish.com>
Removal Link: <https://socialcatfish.com/opt-out/>
Contact: welcome@socialcatfish.com
Notes: Online removal tool will complete the process.

Service: Spy Dialer - <https://www.spydialer.com>
Removal Link: <https://www.spydialer.com/optout.aspx>
Contact: support@spydialer.com
Notes: Online removal tool will complete the process.

Service: Spokeo - <https://spokeo.com>
Removal Link: <https://www.spokeo.com/optout>
Contact: support@spokeo.com, customercare@spokeo.com
Notes: Online removal tool will complete the process.

Service: SpyFly - <https://www.spyfly.com>
Removal Link: <https://www.spyfly.com/help-center/remove-info>
Contact: support@spyfly.com
Notes: Send email requesting removal.

Service: Spytox - <https://www.spytox.com>
Removal Link: https://www.spytox.com/opt_out
Contact: hello@spytox.com
Notes: Online removal tool will complete the process.

Service: State Records - <https://staterecords.org/>
Removal Link: <https://infotracer.com/optout/>
Contact: support@staterecords.org
Notes: Online removal tool for InfoTracer will complete the process.

Service: Super Pages - <https://www.superpages.com>
Removal Link: https://www.whitepages.com/suppression_requests
Contact: support@superpages.com, info@superpages.com
Notes: "Remove from Directory" at the footer of the page

Service: Sync Me - <https://sync.me>
Removal Link: <https://sync.me/optout/>
Contact: ken@sync.me
Notes: Online removal tool will complete the process.

Service: Telephone Directories - <https://www.telephonedirectories.us/>
Removal Link: https://www.telephonedirectories.us/Edit_Records
Contact: <https://www.telephonedirectories.us/Contact>
Notes: Online removal tool will complete the process.

Service: Tenn Help - <https://www.tennhelp.com>
Removal Link: <https://www.tennhelp.com/public-resources/change-listing.html>
Contact: <https://www.tennhelp.com/public-resources/contact-us.html>
Notes: Online removal tool will complete the process.

Service: That's Them - <https://thatsthem.com>
Removal Link: <https://thatsthem.com/optout>
Contact: Unknown
Notes: Online removal tool will complete the process.

Service: Thomson/Westlaw/CLEAR - <https://thomson.com>
Removal Link: None
Contact: west.privacypolicy@thomson.com
Notes: Send email with removal request.

Service: TLO - <https://tlo.com>
Removal Link: None
Contact: CustomerSupport@TLO.com, TLOxp@transunion.com
Notes: Send demand via email to remove all records. Expect resistance.

Service: Tower Data - <https://www.towerdata.com>
Removal Link: dashboard.towerdata.com/optout/
Contact: privacy@towerdata.com
Notes: Online removal tool will complete the process.

Service: True Caller - <https://www.truecaller.com>
Removal Link: <https://www.truecaller.com/unlisting>
Contact: support@truecaller.com, info@truecaller.com
Notes: Online removal tool will complete the process.

Service: True People Search - <https://www.truepeoplesearch.com>
Removal Link: <https://www.truepeoplesearch.com/removal>
Contact: <https://www.truepeoplesearch.com/contact>
Notes: Online removal tool will complete the process.

Service: True People Search.net - <https://www.truepeoplesearch.net>
Removal Link: <https://www.truepeoplesearch.net/removal>
Contact: <https://truepeoplesearch.net/contact.html>
Notes: Online removal tool will complete the process.

Service: Truth Finder - <https://www.truthfinder.com>
Removal Link: <https://www.truthfinder.com/opt-out/>
Contact: support@truthfinder.com
Notes: Online removal tool will complete the process.

Service: UFind - <https://ufind.name>
Removal Link: None
Contact: support@ufind.name
Notes: Send email with removal request. Removes data from several subsidiaries.

Service: United States Phonebook - <https://www.unitedstatesphonebook.com/>
Removal Link: None
Contact: paulmfield@gmail.com - lookupuk@gmail.com
Notes: Send email with removal request. Removes data from several subsidiaries.

Service: USA People Search - <https://www.usa-people-search.com>
Removal Link: <https://www.usa-people-search.com/manage/>
Contact: <https://www.usa-people-search.com/contact.aspx>
Notes: Online removal tool will complete the process.

Service: US Phonebook - <https://www.usphonebook.com>
Removal Link: <https://www.usphonebook.com/opt-out>
Contact: support@usphonebook.com
Notes: Online removal tool will complete the process.

Service: Valassis/RetailMeNot/Redplum - <https://www.retailmenot.com>
Removal Link: <https://www.retailmenot.com/privacy/do-not-sell-my-info>
Contact: <https://help.retailmenot.com/s/contactsupport>
Notes: Online removal tool will complete the process.

Service: Valid Number - <https://validnumber.com/>
Removal Link: None
Contact: <https://validnumber.com/doc/contact/>
Notes: Send removal request through contact page.

Service: Valpak/Cox - <https://valpak.com>
Removal Link: <https://www.valpak.com/coupons/show/mailinglistsuppression>
Contact: info@skulocal.com
Notes: Online removal tool will complete the process.

Service: Vehicle History - <https://www.vehiclehistory.com>
Removal Link: None
Contact: support@vehiclehistory.com
Notes: Email requesting removal.

Service: Veripages - <https://veripages.com>
Removal Link: <https://veripages.com/page/contact>
Contact: support@veripages.com
Notes: Send email with removal request.

Service: Verispy - <https://www.verispy.com/>
Removal Link: <https://www.dataaccessmanagement.com/verispy/>
Contact: support@verispy.com
Notes: Online removal tool will complete the process.

Service: Veritora - <https://veritora.com/>
Removal Link: <https://federal-data.com/control/profile?url=>
Contact: <https://federal-data.com/page/contact>
Notes: Paste your original url from veritora.com following the = sign in the removal link.

Service: Visa - <https://visa.com/>
Removal Link: <https://marketingreportoptout.visa.com/OPTOUT/request.do>
Contact: None
Notes: Online removal tool will complete the process.

Service: Voter Records - <https://voterrecords.com/>

Removal Link: <https://voterrecords.com/faq>

Contact: <https://voterrecords.com/contact>

Notes: Follow directions in the FAQ above.

Service: Westlaw - <https://www.thomsonreuters.com>

Removal Link: https://static.legalsolutions.thomsonreuters.com/static/pdf/opt_out_form.pdf

Contact: westlaw.privacypolicy@thomsonreuters.com

Notes: Print form, complete, and mail to listed address. Include extended opt-out form.

Service: White Pages - <https://whitepages.com>

Removal Link: https://www.whitepages.com/suppression_requests

Contact: support@whitepages.com

Notes: Online removal tool will complete the process.

Service: Whooster - <https://www.whooster.com>

Removal Link: None

Contact: privacy@whooster.com

Notes: Send email with removal request.

Service: WYTY - <https://wyty.com>

Removal Link: <https://www.wyty.com/remove/>

Contact: privacy@wyty.com

Notes: Online removal tool will complete the process.

Service: XLEK - <https://www.xlek.com/>

Removal Link: <https://www.xlek.com/optout.php>

Contact: <https://xlek.com/contact.php>

Notes: Online removal tool will complete the process.

Service: Yasni - <https://yasni.com>

Removal Link: None

Contact: info@yasni.com, support@yasni.com

Notes: No removal option, but will identify sources of data. Will refresh occasionally.

Service: Yellow Pages - <https://www.yellowpages.com/reversephonelookup>

Removal Link: <https://corporate.thryv.com/privacy-CCPA>

Contact: ypcsupport@yp.com, press@yp.com

Notes: Online removal tool will complete the process.

Service: Zabasearch - <https://zabasearch.com>

Removal Link: None

Contact: info@zabasearch.com, response@zabasearch.com

Notes: Send your custom opt-out request form via fax to 425-974-6194.

Service: ZoomInfo - <https://zoominfo.com>

Removal Link: <https://www.intelius.com/opt-out>

Contact: info@zoominfo.com, support@zoominfo.com

Notes: Online removal tool will complete the process.

Search Engine Re-Indexing

Anytime you remove information from the internet, whether it is from people search websites or the methods explained later in this chapter, you should submit the target websites for re-indexing through the major search engines. Otherwise, sensitive data might still be included within a search result for your name, even though the content has been removed from the source website. As I write this, a client has asked me to remove her home address displayed on a website. I was successful. However, a Google search of her name links to this site and displays her home address within the summary below the result. I need Google to re-index the website in order to remove the entry from this search.

- Sign in to any Google account.
- Navigate to <https://search.google.com/search-console/remove-outdated-content>.
- Click “New Request”.
- Enter the exact URL of the target page.
- When prompted, enter a word that appears in the old version but is no longer live.
- Submit the request.

In my scenario, I entered the street name which was present before removal. Google confirmed that their search index had indexed this word on that URL and that the word was no longer present. After 24 hours, a search for my client’s name no longer presented this result. We can replicate this process with Bing.

- Sign in to any Microsoft or Google account.
- Navigate to <https://www.bing.com/webmasters/tools/contentremoval>.
- Enter the exact URL of the target page.
- Select “Remove outdated cache”.
- Submit the request.

Data Removal Shaming

In 2019, I began seeing more people search websites shaming those who have requested removal from their service. Consider the “Removal Error” page located on the Locate Family website at <https://www.locatefamily.com/removal-errors.html>. It publicly displays every person who requested removal while using a disposable or temporary email address. Not only did Locate Family refuse to remove the profiles, they announced to the world anyone who tried to protect their privacy by using a masked email provider. This is deliberately malicious and an attempt to shame anyone craving privacy. We must always be cautious of these abuses. If a site refuses to remove profiles because a masked email was used, we may need to assign a ProtonMail account for this purpose.

Social Media Background Services

In 2020, I began seeing more companies providing a service to report “inappropriate” workplace behavior as an employee screening strategy. If you are about to hire a person at your business, these companies will provide a complete report of online activity from the potential employee. This includes any social network posts which contain profanity or threats of violence. Unfortunately, these systems also collect posts with no inappropriate content. This is especially true with posts containing humor and sarcasm taken out of context.

One of the offenders in this game is FAMA (fama.io). It appears that they collect any publicly available social network content which displays “toxic behavior” and stores it indefinitely. When a potential employer requests this service and provides any identifiers about the employee, FAMA conducts a query and provides any content gathered about the individual. This usually includes posts which the employee “liked” which happen to contain a curse word. This seems quite excessive to me. If you identify any of these services in use by your potential employer, you might consider removing your data before the background check. Below are a few options for the most popular services.

- **FAMA:** Send an email to privacy@fama.io and specifically demand removal of any data stored in reference to your social network account(s).
- **Social Intelligence:** Send an email to info@socialintel.com or call 888-748-3281 and demand removal of any data stored in reference to your social network account(s).
- **JDP:** Send an email to clientservices@jdp.com or call 877-745-8525 and demand removal of any data stored in reference to your social network account(s).
- **Good Egg:** Send an email to privacy@goodegg.io and demand removal of any data stored in reference to your social network account(s).
- **Ferretly:** Send an email to info@ferretly.com and demand removal of any data stored in reference to your social network account(s).
- **Critical Research:** Send an email to privacy@criticalresearch.com and demand removal of any data stored in reference to your social network account(s).
- **A Good Employee:** Send an email to customerservice@agoodemployee.com and demand removal of any data stored in reference to your social network account(s).
- **Background Profiles:** Complete the online contact form, demanding removal of any personal data stored, at backgroundprofiles.com/contact-us/.

If any of these companies refuse to honor your removal request, consider an additional attempt citing the California Consumer Privacy Act, as explained soon.

Mailing List Removal

If you have removed yourself from all of the people search websites and forwarded all of your personal mail to a CMRA or PMB box, you are still likely to receive some junk mail in your true name at your home. This can be frustrating and is a sign that your personal information will continue to populate online websites. I encourage you to eliminate all mail in your name, even if it is meaningless advertising. I offer a few thoughts when a company refuses to remove you from their database.

Demanding absolute removal typically fails. Companies do not want to lose potential future business. Therefore, I find a request for change of address works better. I call the company and tell them that I just moved and no longer receive updates about their products. I advise that I want to update my address in their database. I then provide my true home address which is still receiving the mail and claim that I have moved. I provide a street address of a real apartment complex, but an apartment number which does not exist.

If this method fails, I claim death. I send an email similar to the following.

"I'd like to cancel a subscription to your catalog. The original subscriber was my mother and she has recently passed. The catalogues are upsetting my father."

Most companies will cancel the mailings immediately, and often apologize for the inconvenience. Some readers may scoff at my strategy. Please remember that I only recommend this after polite requests to be removed are ignored by the company.

We also have the option of DMAChoice's Deceased Do Not Contact List (DDNC). The contact information for "deceased" individuals can be entered into their mail, telephone and email preference services and offered as a stand-alone file so that marketers can suppress them from marketing lists. Any provided details will be flagged so marketers will be able to remove those specific names from their prospect marketing lists. The form is available at the following location and further details about the services of DMAChoice can be found within the second address.

<https://www.ims-dm.com/cgi/ddnc.php>
<https://www.dmachoice.org/>

Finally, Direct Mail offers a "National Do Not Mail List", but I have yet to witness any effectiveness. More details can be found at the following address.

https://www.directmail.com/mail_preference/

California Consumer Privacy Act

In 2020, the California Consumer Privacy Act (CCPA) became effective, which is a state statute intended to enhance privacy rights and consumer protection for residents of California. However, residents of other states may also benefit from this law. First, let's summarize the basic characteristics of the CCPA. Overall, it grants California residents the following three basic rights in association to their relationships with businesses.

- KNOW what personal information companies possess about you.
- DELETE your information if desired.
- DEMAND companies not to sell your information.

This may sound powerful, and it is, but there are always caveats. First, you must be a California resident in order to be eligible for protections from this law. However, many companies with a strong California presence, such as Facebook, Google, Microsoft, and others are applying the protections to all customers regardless of location. Next, there are exemptions which companies can use to refuse your requests, including the following.

- The data is necessary to complete transactions.
- The data is necessary to comply with legal obligations.
- The data is necessary to protect security and functionality.
- The data is necessary to protect free speech.
- The data is necessary to complete scientific research.
- The data is necessary to complete internal uses.

It would not take much effort for a company to apply one of these exemptions to your request. However, it is always worth trying. In early 2020, I encountered a website which refused to remove sensitive personal information from their publicly available online service. I sent the following request to the email address on their website.

Pursuant to the California Consumer Privacy Act (CCPA), I demand that my personal information be removed from your website. Furthermore, per Part 4 of Division 3 of the California Civil Code (AB-375), I demand a waiver of any payment for this demand. My current California address is as follows.

Michael Bazzell
GENERAL DELIVERY
Los Angeles, CA 90001-9999

The company did not respond, but my information was removed the next day. They could have likely claimed an exemption, but it is less effort to simply remove content. It is also not worth the risk of violating the CCPA, as each violation carries a \$2,500 - \$7,500 penalty. This only applies when the company generates more than \$25 million per year in revenue; collects information on more than 50,000 consumers each year; or derives more than 50 percent of its annual revenue from data. This should be applicable to most services which possess threats to our privacy.

I highly doubt the company displaying my details sent anything to the address I provided, but it is legal for me to use it. This address is the General Delivery option for Los Angeles, and any mailings will be forwarded to the post office located at 7101 South Central in Los Angeles. I would need to respond to that location with ID in order to pick up any general delivery mail. This should never be used whenever a package will be sent. I only use it as a temporary California address. I feel this is acceptable, as the official USPS website states "General Delivery is a mail service for those without a permanent address, often used as a temporary mailing address". Since my home is in the name of a trust, of which I am not the trustee, I believe I technically do not possess a "permanent mailing address". My PMB and UPS box would go away if I failed to renew either, so I view those as "temporary". I am probably unnecessarily splitting hairs here, but I like to have a clean conscience while executing my strange tactics.

The CCPA defines protected personal information as any data including the following.

Real Name	Passport Number
Alias Name	Purchase History
Postal Address	Biometric Information
Email Address	Browsing History
Online Identifier	Search History
IP Address	Geolocation Data
Account Name	Professional Information
Social Security Number	Educational Information
Driver's License Number	

This provides many opportunities for privacy seekers. Any time you identify a company possessing or selling this type of data about you, you might be able to demand them to stop. Each scenario will be unique, and you should expect resistance. I suspect we will see other states follow in California's footsteps. Ideally, we would see a federal law provide similar protections, but that is likely much more complicated than each state taking charge for their residents.

The United States Census

It may be useless documenting these strategies now, since we just experienced a census in 2020. The next tally of every resident in the country will not occur until 2030. However, we should have a conversation in the case that your neighborhood, city, county, or state decides to conduct their own investigation into the population within specific boundaries. A census is defined as the procedure of acquiring and recording information about the members of a given population. In simplest terms, the U.S. Census attempts to identify the primary residence of every resident as of April 1st every ten years.

The Census bureau will tell you that the responses are confidential and secure. The intentions are good, but we know the history of the government failing to protect our data, such as the OPM breach. They will want to know the full name, DOB, gender, and relationship of every person in your household. This may seem harmless, but we must use caution. If the Census bureau were to experience a data leak or breach, this content would be extremely valuable to the people search websites previously mentioned. If you applied the techniques in previous chapters in order to remove any association from your home to your name, you may be hesitant to hand these private details over to the government. Since it is federal law that you accurately complete the census form, there is no option to simply ignore this demand. If you do, expect Census employees to start knocking on your door demanding answers. Our goal is to stay off their radar, and not bring attention to ourselves.

However, you can comply with the Census while maintaining a sense of privacy. When you receive a form requesting the name, gender, and DOB of every resident of the home, I believe you can legally comply by responding similar to the following in the name fields.

Adult Male
Adult Female

Minor Male
Minor Female

This provides the number of occupants, gender, and whether each person is an adult or minor. This gives the Census enough data to continue their tally in order to provide appropriate services, grants, and various government programs to your area. If you do this, there is always a possibility that an employee will be unsatisfied with your answers and may still contact you to seek more information. I encourage you to include a VOIP telephone number on the form. This may encourage the employee to call instead of visiting in person. Most importantly, never lie on these forms or ignore them. This is not an opportunity to provide disinformation. Doing so may result in a steep fine.

Online Content Removal

Bad things happen. I know people who have spent many months creating their perfect invisible life only to see it jeopardized by one minor mistake. While this will likely never happen to you, it is important to be prepared. This section will provide immediate actions which can be taken to minimize the damage after a mistake or malicious act has caused a data leak. Your scenario will likely fall into one of the following categories.

- A photo or video of you is posted online.
- Your financial information or documents are posted online.
- Your reputation is purposely slandered online.
- Your criminal or traffic charges are posted online.

Personal Photos

If you strive to prevent photos of yourself from appearing online, you are aware of the constant struggle. Family and friends are constantly updating their Facebook, Twitter, and Instagram feeds with photo and video proof of every facet of their lives. There are no opt-out policies on these websites. There are no removal request forms. Your only option is a polite request.

I have found that a simple request to friends and family is usually sufficient for them to delete any sensitive photos. Unfortunately, there is little else that can be done. I can only recommend that you never take a threatening tone. This will only agitate the person that controls the photo and they may become resistant. I have found one thing in common with the majority of my clients with this problem. Every one of them had been tagged because of their own use of social networks. If you are not on Facebook, you cannot be tagged on Facebook. If you are not on Twitter or Instagram, you are much less likely to be seen on someone else's account.

In late 2015, I presented a keynote session at a large conference in the Caribbean. This 60-minute session focused on cyber-crime vulnerabilities and the ways that criminals use social media information to create sophisticated attacks. An hour later, I received an email from one of my automated alerts which monitor my personal information. An attendee in the audience had taken a photo of me during the lecture and posted it to Twitter. I immediately reached out through a private message and politely requested removal. The attendee agreed and the entire post was removed. This was completed before Google had the opportunity to add it to their images database. If I did not have a monitoring solution in place, which was Google Alerts at the time, I would never have noticed the post. Google and Bing would have indexed the post and image. I would then have a more difficult time removing all traces. Constant monitoring is vital.

Personal Videos

Today, I believe you are more likely to be captured within an online video than a still image. Fortunately, your presence within a video will not always be as obvious as a photo, but you may desire removal of the video exposing your image. This often presents a very difficult situation. In 2020, a client asked me to remove a video which had been posted to YouTube and Vimeo which included audio and video of her engaged in a private conversation during a lecture. This was captured with a hidden camera while my client was presenting a keynote speech inside a hotel conference room.

I knew Vimeo would be the easiest request, so I navigated to their “Privacy Complaint Form” located at <https://vimeo.com/help/violations/privacy>. I completed the form and added the following within the comment field.

“This video, including my name, voice, and likeness, does not have my consent to be published online. It contains content presented as part of a paid speaking engagement which is not authorized for public distribution. Please provide proof of consent from the original uploader or remove the video.”

Within 48 hours, Vimeo responded stating that the uploader refused to respond to the request for proof of consent and that the video had been removed. This was expected from Vimeo, but I knew YouTube would be a bigger issue. I began the “Privacy Complaint Process” through Google at <https://support.google.com/youtube/answer/142443> and repeated the claim of infringement on behalf of my client. Within 24 hours, I received the following email from Google.

“It has been brought to our attention that activity in your account may violate YouTube’s Terms of Service. After review, we have determined your account is not in compliance with our Terms of Service and have terminated your account accordingly. Please be aware that you are prohibited from accessing, possessing or creating any other YouTube accounts. For more information about account terminations and how our Community Guidelines are enforced, please visit our Help Center. If you would like to appeal the suspension, please submit this form.”

In other words, Google terminated my account for filing a complaint. I filed an appeal but never heard anything back from them. I present this as a warning. Google will not only refuse your privacy invasion, regardless of the scenario, but they will also terminate your account preventing access to any of your content. The video is still present on YouTube, but it is buried under dozens of social network profiles, blog posts, personal web pages, and other neutral content created for this purpose.

Revenge Pornography Photos and Videos

I constantly receive email messages asking for help with removal of slanderous content. This is usually from business owners trying to protect their brand; individuals wrapped up in online gossip; or parents attempting to shield their children from bullies. If someone simply states an opinion about your product or business online, there is nothing you can do. If someone is spreading rumors about you on social networks, no one will take your complaint. If you find malicious comments about your child online, you can only report it to the host of the content. However, there are a few “tricks” which can force content offline.

In 2015, I was contacted by a woman who was suffering from a bad case of stalking. Her ex-boyfriend constantly harassed her and her new boyfriend online. He posted malicious content on various websites and referenced them both by full name. He had posted so much content that some of it had made it to the front page of a Google search. At one point, the first result after searching her name was a pornographic video fictitiously claiming to be her. She had enough and wanted to take action.

These cases are sometimes difficult to tackle because of laws that protect free speech. I am obviously a big fan of the first amendment, but I also believe that one has a right to take advantage of other laws and policies in order to protect a reputation. My goal was to eliminate all malicious content from the first page of both a Google and Bing search. The following highlights my successes and failures.

The first website on her Google and Bing search results was a revenge pornography page. It displayed a pornographic video of an unknown female (not the victim) who appeared to be asleep on a bed. An unknown man (not the suspect) then sexually molests the woman while she sleeps. It should be noted that this video was likely staged and the woman was probably a willing participant. These consensual videos have become popular on commercial pornography websites. The title of the video on this page included my victim's full name. The comments made several references to her, the new boyfriend, and her family. I believe that the former boyfriend wanted the world to think that the woman in the video was my victim. They did appear very similar physically.

Removing this first link was relatively simple. I first navigated to the official Google revenge porn reporting page at support.google.com/websearch/troubleshooter/3111061. I selected the following options, each of which appeared after the selection of the previous.

What do you want to do? Remove information you see in Google Search
The information I want removed is: In Google's search results and on a website
Have you contacted the site's webmaster? Yes, but they haven't responded
I want to remove: A pornographic site that contains a full name or business name

Does the page contain pornographic content? Yes

Does a full name or business name appear on the website without your permission? Yes

Does the page violate Google's Webmaster Quality Guidelines? Yes

I then supplied an alias email address that I created for the victim; the full name of the victim as it appeared on the web page; the address of the Google result page linking to the video; and the address of the actual video page. I submitted the request and moved on to Bing.

I navigated to Bing's simple "Report Content to Microsoft" website located online at <https://www.microsoft.com/en-us/concern/revengeporn>. I provided the victim's name as it appeared on the video page, the exact address of the page, confirmation that the victim did not consent to the posting, and a digital signature.

I received a response from Bing within 24 hours and the link was removed. Google responded over 15 days later and they also removed the link. Both cited their revenge porn policies and gave no resistance to the removal. While the female in the video was not the victim, I believe that identifying the victim as the participant warranted this type of submission. Interestingly, neither service specifically asked if the requestor was actually depicted in the pornographic video. They only required the requestor's name be included on the page.

At this point, the Bing results page was fairly clean. The first page included legitimate LinkedIn and other social network pages under the control of the victim. However, Google was a different story. The suspect had created a post on a popular revenge pornography web forum where he linked to the previously mentioned video. Technically, this video was not present on the website, only mention of it and a direct link. This forum post was now the number one result when searching my victim's name. This page made several references to her full name and identified her in the inappropriate video. I submitted this page through the same Google reporting page and waited. I was denied the request because the page did not contain any actual pornography. The direct link did not satisfy the requirements of their takedown policy.

I took drastic action that would not be appropriate for all situations. This web forum allows any members to post comments about the videos. I created a new member account anonymously, and submitted a comment on the page in question. In this comment, I embedded an animated image in gif format that displayed a very short (partial) clip of the video in poor quality. This clip looped and repeats while people are reading the comment. It did not actually include nudity, only showing unidentifiable bodies from the target video. I resubmitted my request to Google and the link was removed nine days later, as it now violated their terms of service (even though it was my fault). The rest of the results on the first page of her Google search were legitimate websites that she approved. My work was complete.

DMCA Rights and Failures

I once assisted a client when a website which contained extremely personal and slanderous details about her refused to remove the content. The theme was that she was a cheater and it included false accusations of infidelity. She suspected it was published by her former boyfriend, as it appeared days after their breakup. It was a free WordPress blog hosted on the official WordPress domain. The page contained her full name and several photos of her. My first attempt was a DMCA takedown request, which failed.

DMCA is an acronym for the Digital Millennium Copyright Act. It is a U.S. copyright law. It addresses the rights and obligations of owners of copyrighted material who believe their rights under U.S. copyright law have been infringed, particularly on the internet. DMCA also addresses the rights and obligations of OSP / ISP (Online / Internet Service Providers) on whose servers or networks the infringing material may be found.

My client confirmed that she possessed the original photographs which appeared on the website. Some of them were captured with her own mobile device, and her originals could prove this. In my view, she was the copyright holder of these images. WordPress was violating this since she did not authorize the publication of the photos. WordPress has an easy DMCA submission page at <https://en.support.wordpress.com/our-dmca-process/>. I followed the steps and issued my complaint. The next day, I received the following message.

“We have reviewed your DMCA notice and the material you claim to be infringing. However, because we believe this to be fair use of the material, we will not be removing it at this time. Please note that Section 107 of the copyright law identifies various purposes for which the reproduction of a particular work may be considered fair, such as criticism, comment, news reporting, teaching, scholarship, and research. Please note that you may be liable for damages if you knowingly materially misrepresent your copyrights – and we may seek to collect those damages.”

Not only did WordPress deny my claim, they threatened to seek damages from my submission. I am sure this is a canned response due to abuse, but I found it a bit inappropriate. My next attack was on the suspect blog itself. The page allowed anonymous comments below the slanderous content. I scribbled a barely legible signature on paper, took a photo with my anonymous mobile device, and uploaded it to the page. It immediately appeared, as the site did not require administrative approval for new posts. I then submitted the page to Google for takedown, as explained in the following page. Per their policies about websites containing signatures, the site was removed from their index within a week. The original page is still present on WordPress, but no one searching for my victim on Google or Bing will find it.

Financial Information

If you find a page in a Google search result that displays personal information about you, such as your social security or credit card number, you can request immediate removal. Google will review the request and remove the information from their search results. This will not remove the information from the website that is displaying it, but it will take the link off Google to make it more difficult to find. Even if Google removes the link from their search results, you should contact the offending website directly and request removal of your information. The following are the three scenarios that will force Google to remove a link to personal information.

- Your Social Security Number is visible on a website.
- Your bank account or credit card number is visible on a website.
- An image of your handwritten signature is visible on a website.

Each of these situations can be reported through the following three specific websites.

- support.google.com/websearch/contact/government_number
- support.google.com/websearch/contact/bank_number
- support.google.com/websearch/contact/image_of_handwritten_signature

Each page will instruct you to complete an online form which requires your name, anonymous email address, the URL of the website that is exposing the information, the URL of a Google results page that displays the information, and the information being exposed. Fortunately, Google offers detailed help on these pages explaining how to obtain the required information.

Bing also offers an automated removal request with an option of “My private information (intimate or sexual imagery, credit card numbers, passwords)”. This form can be found at the following website.

<https://www.microsoft.com/en-us/concern/bing>

In early 2015, I was contacted by an attorney that was attempting to remove some content from the internet. He and a former business partner had developed a nasty relationship after a failed venture. The former partner uploaded numerous sensitive contracts on which he claimed my client had defaulted. He placed them on his personal website and posted malicious comments about my client. Since my client had a very unique name, a Google search revealed this undesired information within the first three results. At first, I assumed that there was nothing I could do about this expression of free speech. The documents were legal.

However, each scanned contract on this website included the signature of my client. I submitted a request to Google for removal of the link to this website. I cited their policy about linking to images of a person's signature. Within five days, the link was gone. While the presence of a signature was not the concern of my client, I used it as leverage to remove the undesired content. Sometimes you may need to look at alternative ways to achieve your desired removal results.

If you want to know whether your signature, social security number, credit card number, or bank account information is visible on a public website, you will need to conduct specific searches. The easiest way is to occasionally conduct a search of your account numbers and view any results. Keep in mind that your searches will only be successful if the exposed data is in the same format of your search. Also, use an anonymous search option such as the website duckduckgo.com. You should conduct several searches of this type of data including spaces, without spaces, and only the last four or eight numbers alone. This also applies to searches for any financial account numbers and social security numbers.

Libelous Websites

There is a disturbing new trend of websites which allow anonymous users to post any type of slander about an individual or company. These include services such as Ripoff Report and cheating spouse websites. Remember, it is not vital to always remove the CONTENT. It is more important to remove the LINK to the content from search engines. This is how people are likely to find the sites you want removed. I won't go to every website and look you up, but I will go to Google and follow any links. Therefore, I target the most likely source viewed by someone. Let's discuss complaint websites such as Ripoff Report as an example.

This website allows users to complain anonymously about any company or person. It requires users to create an account before reports can be submitted, but it does not verify the identity of users. Ripoff Report results usually show up on Google searches for the people or companies mentioned in the report, which can be embarrassing or damaging. According to the site's Terms of Service, users are required to affirm that their reports are truthful and accurate. However, the site says that it neither investigates, confirms, nor corroborates the accuracy of any submissions. In other words, it is an easy way to get revenge against an adversary.

Companies or individuals who have been named in a report may respond with a rebuttal. There is no charge to submit one, but they must have a registered account. The rebuttals are almost never successful in removal of information. Alternatively, to repair the reputation because of something that is written in the website, Ripoff Report asks victims to pay high fees for internal investigations of complaints and responses carried out by Ripoff Report's

pool of arbitrators. Another way of phrasing this is “extortion”. Again, these investigations almost never result in the desired removal.

How bad can these sites be? On Ripoff Report, I see entries about my clients falsely accusing them of fraud, adultery, theft, and in one instance murder. Anyone can post anything they want without any accountability or fear of prosecution. It is a cesspool of hate. Worse are the “cheating” sites such as shesahomewrecker.com. These sites allow anyone to anonymously report a “cheater”, including photos, full names, addresses, and explicit descriptions. These sites are a popular magnet for people desiring revenge, regardless if the other person has done anything wrong. There are also numerous websites that allow anonymous reporting of people that have a sexually transmitted disease (STD). For obvious reasons, I will not provide a link. Overall, there are many places where people can ruin digital lives quickly. Imagine if a Google search for your name instantly revealed a website announcing you have an STD. Clients call me constantly asking for help with these situations.

The best solution I have to offer is to attack through the legal system. Suing the websites is not likely to work in your favor. Many are hosted overseas, and all will claim protection by the 1996 Communications Decency Act which provides immunity from liability for providers and users of an “interactive computer service” who publish information provided by third-party users. In other words, I can host a website and not be held liable if someone else posts something defamatory.

Instead, I have initiated lawsuits in order to obtain a court order to remove online links to defamatory content. Google and Bing will not respond to my request to remove hateful content. Google may agree with me that the post is inappropriate, but that means nothing. They will only respond to a specific court order. Therefore, the first step is to get a judge to issue the order. However, that first requires a lawsuit. If you do not know the identity of the suspect, it can be difficult to launch a civil case. This is where a “John Doe” or “Fictitious Defendants” lawsuit can be a powerful tool.

Assume that Ripoff Report possesses an anonymous report about you. It clearly displays false defamatory content that has created a “loss” for you. Maybe you applied for a job and did not get it, and you believe it is from the posting. Maybe you have lost business because of the content. You may have significant losses which you can cite in court as damages. You file a fictitious defendant civil lawsuit at your local court due to the defamation and potential damages. This provides you subpoena power. You can now request a subpoena to the websites that possess the content with hopes of identifying the culprit via IP logs or email addresses. This identification rarely happens, but it places pressure on the sites and their legal teams.

Next, you can petition the court to provide an official court order to remove the content from the internet. The wording of this can vary, and must be precise to your situation. Be sure that

the order forces removal of all links to the specified content and any cached copies. The offending sites will ignore this request, but Google will not. Upload the entire court order to Google at support.google.com/legal/contact/lr_courtorder?product=websearch.

Expect no response at first, and submit the same order once weekly until the links have been removed. Some courts will send the order on your behalf, which usually results in a faster removal. I have seen content removed within 48 hours and up to two weeks later. In most states, your right to file a defamation lawsuit ends a year after the initial publication, including original internet posts. In my experience, a John Doe suit can cost \$5,000 to \$15,000 in legal fees. Consult with an attorney to determine the relative merits and potential of success for your specific case. It is possible to do all of this yourself, but it is not advised. Any mistake can ruin your chances of an order being signed by a judge.

This court order is often in the form of a Cease and Desist order (not a letter). An order is created by the court, and a letter would be created by you. Cease and Desist letters are almost always ignored, but a court order is not. This universal document can be used in many scenarios, such as copyright infringement, trademark infringement, debt collection, harassment, slander, and libel. These orders vary widely between states, counties, and judges. Because the order is issued by the judge presiding over your civil case, you must convince him or her to issue the order, and to include the desired wording. This is where a well-known local attorney can be very valuable.

Any valid Cease and Desist court order should include descriptions of each false statement, reasoning why the statements are false, and descriptions of how the false statements affect you. You must clearly claim that you have damages from the published content. Without this, there is very little need for a civil suit. I have had clients who have been able to substantiate financial loss, even if minimal, from the undesired content. It will be up to you to determine if you have suffered any loss. The following page contains a fictitious example of a court order demanding Google to cease and desist providing access to libelous content. It is not a template or actual document, and is presented only for understanding of the technique.

Assume that you own a carpet cleaning company, and one of your competitors posted on Ripoff Report stating you were a criminal and possessed STDs (this is a common theme with libelous online complaints). The order on the following page would tackle this and demand that Google remove the links to this content.

I have over-simplified the process of filing a lawsuit and obtaining a court order. This is where a proficient attorney can assist greatly. I never attempt any of this myself. I always hire a local attorney on behalf of my client. I usually seek former prosecutors who understand the system and have direct access to judges.

CEASE AND DESIST ORDER

[The Honorable Judge John Doe]
[City, State, Zip Code]
[Date]
VIA Certified Mail

Google Inc.
Legal Compliance
1600 Amphitheatre Parkway
Mountain View, CA 94043

RE: Cease and Desist – Libel

To Whom It May Concern:

It has come to my attention that your company is currently providing direct access to specific online content contested as libelous to [YOUR NAME]. A direct link to the libelous website is available on your service when searching [YOUR NAME]. The exact address of this content is currently located at <https://www.ripoffreport.com/reports/carpet-cleaning-by-psycho>. The content on this page states in part:

"[YOUR NAME] is now facing multiple criminal and civil actions including investigation by the IRS and FBI for failure to pay taxes, impersonating a federal agent, making false claims, animal abuse, slander, fraud, stalking and collecting welfare funds while claiming no source of income. He is a pervert and has several STDs."

[YOUR NAME] contests these statements as false during current civil litigation. [YOUR NAME] has no known criminal record and there is no known evidence available to this court substantiating the additional claims made on this site. [YOUR NAME] claims economic harm as a result of the online content that your company provides during a search of the name [YOUR NAME]. [YOUR NAME] claims potential loss of income due to potential employers identifying this content during a search of [YOUR NAME].

I hereby demand that you immediately cease and desist displaying any hyperlinks, including any cached content, to the above referenced website(s) within 10 days of the date of this letter, and notify me in writing when these tasks have been completed.

Judge John Doe

Criminal Information

Many new websites have appeared which host mugshots and associated criminal information of anyone arrested in select states. This varies based on state laws which allow unlimited access to this type of content. While arrest records are public data, I do not support websites that post this data in bulk. They are not doing this as a public resource. They are extortion websites which hope to benefit from your removal request. Most of these will remove your mugshot for \$500. The only purpose for these sites is for financial gain.

I have found removal requests to these websites to be a waste of time. Letters from lawyers will go unanswered. They simply do not care. If your mugshot appears on one of these sites, I have only found two potential solutions. Your results will vary with this technique. The following examples will explain the processes that I took for two clients.

I was contacted by a subject who had been arrested for speeding. This may sound ridiculous, but he was speeding over 20 miles per hour above the limit, which was a misdemeanor in his state. He was booked, processed, and released on bond. The next day, his mugshot appeared on one of these extortion sites. Within a week, it had been indexed by Google. A search of his name revealed the mugshot directly above his LinkedIn and business websites. He was devastated.

The website that hosted this image was fairly dysfunctional. It was poorly designed and only existed to make a quick buck. I placed an alert on the exact page where the client's information was hosted through a service called Visual Ping. The moment that the website went down for maintenance, I received an alert that the page had changed. I immediately submitted a request for Google and Bing to re-index the client's mugshot page, which was offline. I identified the address as missing, and both Google and Bing re-indexed it during the 24-hour maintenance down-time.

The mugshot was no longer listed in his search results. If someone were to search the website directly, they could still see the photo. This is highly unlikely. It is possible that Google and Bing could re-index this live data. I have found that this usually happens when new content is posted. Since I informed the search engines that the content was missing, it will not immediately re-index that stale data.

I want to clarify that I was very lucky in this scenario. I took advantage of the situation. It is not a permanent solution, but it did buy some time to make an intentional decision that is not based on frantic thinking. I take a firm stance against paying the removal fees offered by these sites. Not only does it give in to this type of behavior, but it also increases the chance of the photo reappearing. If you paid once, you will likely pay twice. Furthermore, most of these websites are owned by the same entity.

The second solution takes advantage of new state laws specifically targeting mugshot websites. Lucky for nomads of South Dakota, this state possesses strong laws that demand these sites remove your content at your request. Send a certified letter to the website stating your demand to remove your mugshot from the website. Advise that this must be completed within 30 days, per South Dakota state law (or your state). Expect this demand to be ignored. After the 30 days have passed, a small claims suit against the offending website should be considered. In my experience, this causes the website to remove the content in order to avoid a costly court appearance. They will know they are in violation of law and rarely submit any resistance.

Right to be Forgotten

The right to be forgotten is a concept that was discussed and put into practice in the European Union and Argentina in 2006. Search engines began to acknowledge this option in 2014. The issue has arisen from desires of individuals to determine the development of their life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past. Basically, you have the right to “start over” in Europe. This does not apply to Americans.

Google and Bing both allow you to submit requests for content removal from search engines if you live in Europe. The removal forms can be found on their support pages similar to the instructions mentioned in the previous example. They will ask for the search results URL and a digital signature of your name. They will verify that your name appears in the results and remove anything defamatory from the index.

Until recently, I found that submitting a request from an email address that possessed a UK domain was sufficient as proof of citizenship. However, Google has become much stricter and now demands photocopied identification. I have found Bing to be more lenient. I cannot advise you on how to proceed with a request like this if you do not live in Europe. I have received many success and failure stories from other people’s attempts to take advantage of this law.

If your sensitive details are posted anywhere online, it is vital that you act quickly. The internet is a timer counting down until your data is spread onto additional websites. Proper alerts, constant monitoring, and better sharing habits will protect your privacy long term. I respect that we cannot control the internet and that removing personal data is like playing cat and mouse. However, I take my privacy seriously. I am willing to put in the effort in order to maintain my desired level of anonymity. Even as an author and international speaker, I keep a low profile online. I have multiple websites, but none connect to my home address or telephone number. I have a business Twitter account, but no posts mention anything about my personality, interests, or location.

Credit Freeze

Over the past ten years, I have conducted numerous presentations about digital crime to global audiences. The one question that I am asked more than any other during these events is "Should I purchase an identity protection service?". While this is a personal decision, I always disclose that I do not subscribe to any of these services. I have had a credit freeze for several years, and do not require expensive identity protection. I believe that those who have a credit freeze in place should not worry about their identity being stolen. Furthermore, I think that a credit freeze is better than the best identity monitoring product that will ever exist. I believe that every U.S. citizen should consider one. I will explain the submission process in a moment.

Protecting Your Credit Accounts & Debit Cards

If a criminal wants to get your money quickly and easily, he or she will target your debit and credit cards. Before the popularity of the internet, this required physical access to your wallet or purse. A victim would know right away that a card should be canceled and the damage would be minimal if caught early. A criminal would risk capture by attempting charges on the cards in person. Today, possession of your cards is not necessary. The internet has created a new avenue to obtain and spend the money in your accounts. This may occur without any indication of problems on your end. This section will present the tools that you need to protect your credit and make you practically invulnerable to identity theft.

Free Credit Report

Before I discuss the techniques that will protect you, you should take a good look at your current credit report. This will identify all of your current open accounts and may identify any problems or fraudulent activity. There are several websites that offer a free credit report. Most of these will try to convince you to sign up for premium offers and never offer an actual free credit report. The only official government-supported and truly free credit report website is at [annualcreditreport.com](https://www.annualcreditreport.com). This website allows you to view your credit report, without any fee, once yearly from each of the three largest credit bureaus. This means that you actually can get three free credit reports every year. Instead of viewing all three reports at the same time, create a schedule to spread out the viewings. I recommend the following.

First, I recommend obtaining your entire credit report from Equifax online at their website <https://www.annualcreditreport.com>. This free report should be used to identify any unknown uses of your identity. If you do not want to submit the request online, you can use the form at <https://www.annualcreditreport.com/manualRequestForm.action> to mail in the submission.

I recommend that you consider closing any unused open credit accounts. The only exception would be whichever account has been opened the longest. If you have an unused account that has been open for ten years without any problems, you may consider leaving that account open. This will help your credit score, whereas closing your oldest account could decrease your score. Closing other unused accounts will provide fewer options for fraud. If you possess a credit line with a local bank that is never used, and that bank experiences an intrusion into their system, you may be victimized for weeks without knowing. The fewer open accounts that you have will result in fewer opportunities for financial fraud. Personally, my priority would be to close any specialty store accounts that you may have opened because of a sales discount, a free promotional item, or a pushy sales person.

Analyze your entire credit report for any errors. Occasional typos are common, and should not create panic. When I first viewed my own report, I discovered that someone else was using my social security number. I was immediately concerned and began to contact the credit bureaus. I quickly discovered that the “suspect” was someone with an SSN almost identical to mine, and someone had mistyped a number at some point. This will happen, and it is not an indication of fraud. You should focus on the open accounts. If you see that you possess a line of credit at an unfamiliar bank, then you should be concerned. If you discover anything suspicious, contact the credit bureau and financial institution to report the potential fraud. They all have a fraud division that will assist with identifying the problem and resolving it. Each situation will be unique and one vague example here would not necessarily apply to you.

You should also contact any financial institution that hosts the fraudulent account and notify them of the issue. You will be mailed paperwork to validate that the account was not opened by you. The process of closing the account will move quickly after that. If you do discover fraud on your credit report, I recommend that you immediately request your report from the other two credit bureaus. This may identify additional fraud that was not listed on the first bureau’s report. If you do not discover fraud, I suggest that you wait a few months before you view the next report. This allows you to continuously monitor your credit throughout the year. Keeping an eye on your credit report is one of the most important tips that I mention in my public speaking appearances.

Credit Opt-Out

Under the Fair Credit Reporting Act (FCRA), the consumer credit reporting companies are permitted to include your name on lists used by creditors or insurers to make firm offers of credit or insurance that are not initiated by you. These are the pre-approved credit and insurance offers that you receive in the mail. They are often physically stolen by street criminals and submitted to receive a credit card in your name at their address. The FCRA also provides you the right to opt-out, which prevents consumer credit reporting companies from providing your credit file information to businesses.

Through the website optoutprescreen.com, you may request to opt-out from receiving such offers for five years. If you want to opt-out permanently, you can print a form that you must send through postal mail. If you choose to opt-out, you will no longer be included in offer lists provided by consumer credit reporting companies. The process is easy.

Credit Freeze Submission

During my training sessions, people often ask about paid services such as Lifelock and Identity Guard. They want to know how effective they are at protecting a person's identity. These services can be very effective, but you pay quite a premium for that protection. A more effective solution is a credit freeze. This service is easy, free, and reversible. A credit freeze, also known as a credit report freeze, credit report lock down, credit lock down, credit lock, or a security freeze, allows an individual to control how a U.S. consumer reporting agency is able to sell his or her data. This applies to six unique credit bureaus (Equifax, Experian, TransUnion, Innovis, Chex, and NCTUE). The credit freeze locks the data at the consumer reporting agency until an individual authorizes permission for the release of the data.

Basically, if your information stored by the credit reporting bureaus is not available, no institution will allow the creation of a new account with your identity. This means no credit cards, bank accounts, or loans will be approved. In many cases if someone tries to use your identity but cannot open any new services, they will find someone else to exploit. I can think of no better motivation to freeze your credit than knowing that no one can open new lines of credit in your name. This does NOT affect your current accounts or credit score.

A credit freeze also provides a great layer of privacy protection. If companies cannot gain access to your credit report, they cannot identify you as a pre-approved credit recipient. This will eliminate many offers mailed to your home. This will also remove you from various databases identifying you as a good credit card candidate. Credit freezes are extremely easy today thanks to state laws that mandate the credit bureaus' cooperation. This section will walk you through the process. Be sure to properly store any PINs provided to you (usually sent via mail) after the successful freezes. You will need this to un-freeze your credit if desired. As of March 2020, Equifax (and possibly others by now) no longer issue a PIN, and rely solely on responses to historical financial questions in order to lift a freeze.

Now that credit reports and freezes are free due to a new federal law, which can be researched at <https://www.congress.gov/bill/115th-congress/senate-bill/2155>, I feel it is time to execute credit freezes in all possible locations. First, submit a credit freeze at the six current credit bureaus via their online submission, telephone, or postal mail options displayed within the following resources. I typically recommend clients begin with the online submission process and move to telephone or postal mail applications if anything is declined (which is common).

Equifax
Online: <https://www.freeze.equifax.com>
By Phone: 800-685-1111
By Mail: Equifax Security Freeze
PO Box 105788, Atlanta, Georgia 30348-5788

Experian
Online: <https://www.experian.com/freeze/center.html>
By Phone: 888-397-3742
By Mail: Experian Security Freeze
PO Box 9554, Allen, TX 75013

TransUnion
Online: https://service.transunion.com/dss/orderStep1_form.page
By Phone: 888-909-8872
By Mail: TransUnion LLC
PO Box 2000, Chester, PA 19016

Innovis
Online: <https://www.innovis.com/personal/securityFreeze>
By Phone: 800-540-2505
By Mail: Innovis Consumer Assistance
PO Box 26, Pittsburgh, PA, 15230-0026
<https://www.innovis.com/assets/InnovisSecurityFreezeRequest-110141767716e41ac7d862e221ac5831.pdf>

Chex
Online:
<https://www.chexsystems.com/web/chexsystems/consumerdebit/page/securityfreeze/placefreeze/>
By Phone: 800-887-7652
By Mail: Chex Systems, Inc. Attn: Security Freeze Department
7805 Hudson Road, Suite 100, Woodbury, MN 55125

NCTUE
Online: <https://www.nctue.com/Consumers>
By Phone: 866-349-5355
By Mail: NCTUE Security Freeze
PO Box 105561, Atlanta, GA 30348

After you have received confirmation that the six credit bureaus have placed a freeze on your credit, navigate back to <https://www.annualcreditreport.com> and request your free credit report from Experian. This report should acknowledge that a freeze is successfully in place. In a few months, repeat the process for Transunion. You are allowed one free report from each of the three providers every year.

Additional Credit Freeze Submissions

Since the publication of the previous edition of this book, several new data mining companies began offering credit freezes. While I believe everyone should consider a freeze with the previous six services, the following options are not as vital. Extreme privacy enthusiasts may desire their identities to be locked to their maximum potential. If you fit into that camp, then the following are for you.

Core Logic: You can obtain a credit freeze at the three services provided by Core Logic, including Credo, Rental Property Solutions, and Teletrack. Core Logic is an emerging provider of credit checks for third parties. I have never needed their services or approval, and likely never will. Therefore, I have frozen my profile within each of their offerings. The following websites will complete the process online.

Credco: <https://credcofreeze.corelogic.com/>

Rental Property Solutions: <https://rpsfreeze.corelogic.com/>

Teletrack: <https://teletrackfreeze.corelogic.com/>

Once a security freeze is in place, Core Logic will provide you with a PIN. Once frozen, your consumer file will only be released when you directly contact Core Logic, provide them with your personal PIN, and request that any information they have on you be released. If you need to lift the freeze temporarily for a period of time, you may request a temporary lift for all third parties by completing the initial request form on the websites mentioned above. Upon submission of your request, you will receive an email from Core Logic, requesting your basic information and your PIN. You can define the length of time you want your consumer file to be available. When that period ends, your files will be frozen again.

TALX: Please consider a freeze of your employment history maintained by The Work Number (Equifax). If any of your current or past employers contracted with this service for employment verification, any details you provided to the company were shared. If your employer did not query this service, you still likely possess a profile which includes your full name, address history, employment history, salary details, and other sensitive information. To place a security freeze on your The Work Number employment report, call them at 800-996-7566 or send a written request via mail to:

TALX Corporation
ATTN: Employment Data Report Dept 19-10
11432 Lackland Road
St. Louis, Missouri 63146

Sagestream: Formerly known as IDA, this company is aggressively entering the credit reporting market. Fortunately, their self-serve online freeze process is immediate and free. Visit <https://www.sagestreamllc.com/security-freeze> to file online or via postal mail. A PIN will be mailed to your verified address and can be used to temporarily lift a freeze if you seek credit from a company querying Sagestream. I have yet to see a need to remove this freeze once enacted.

Advanced Resolution Services: This service allows a temporary lift of a freeze through their website (ars-consumeroffice.com), but the initial request must be received via postal mail. You will need to send the same documentation required by the previous “big six” credit bureaus to the following address. Lately, I see very few companies querying this service, so you might consider skipping this one if you do not feel comfortable disclosing personal details to them.

Advanced Resolution Services
5005 Rockside Rd
Ste 600
Independence, OH 44131

PRBC: My advice here is a bit different from the previous options. I recommend that you first consider whether your data is currently stored by PRBC before taking any action. If you have been notified that smaller bureaus such as Innovis, Chex, or NCTUE do not possess a profile about you which can be frozen, then you may not have a presence at PRBC. If desired, you can request a copy of your credit report stored by PRBC before demanding a freeze. However, they demand unredacted copies of the front and back of your DL. This prevented me from demanding a copy of my data. The required data to freeze your profile is very demanding, and may not be appropriate for those in sensitive situations. Full details of both processes can be found at <https://www.prbc.com/consumer-affairs>.

I cannot stress the importance of credit freezes enough. Anyone with an SSN should submit one right away to all possible options. The new federal law also mandates that any child with an SSN under the age of 16 can also have a free credit freeze. I highly recommend locking down the credit of the entire family.

Several readers have been impacted by the huge breach at the Office of Personnel Management (OPM). Many of you have now received an official notification if your records were part of the breach. If you have ever held a clearance, or applied for one, you are likely a victim. The response from OPM is to offer temporary free credit monitoring. Unfortunately, if you already have a credit freeze in place, you cannot participate in the free coverage. Why? Your credit freeze is blocking the legitimate service from monitoring your activity. I believe that this speaks volumes about the effectiveness of a credit freeze. Aside from hackers, credit monitoring companies cannot see the details of a frozen account. I urge you to never remove a credit freeze in order to allow any free credit monitoring.

Many of these third-party credit monitoring services also induce people to provide even more information than was leaked in the original breach. For example, ID Experts (the company that OPM has paid \$133 million to offer credit monitoring for the 21.5 million Americans affected by its breach) offers the ability to “monitor thousands of websites, chat rooms, forums and networks, and alerts you if your personal information is being bought or sold online”. However, in order to use this service, users are encouraged to provide bank account and credit card data, passport and medical ID numbers, as well as telephone numbers and driver’s license information.

I can see no reasonable purpose for ever giving any company more personal information in order to protect that same data. What happens when they get breached? On a personal note, I was a victim of the OPM breach. I am not worried. I have credit freezes in place, and they have been tested. I have no automated credit monitoring. Am I still vulnerable? Of course, we all are. However, I am a much more difficult target.

Fraud Alerts

In the previous edition of this book, I only placed emphasis on the credit freeze, and did not explain a credit fraud alert. This was intentional, as a freeze is much more powerful than an alert. A freeze prohibits a hard credit check while an alert simply asks a creditor to dig deeper into any requests. In other words, a freeze stops unauthorized credit pulls while a fraud alert slows them down. In 2020, I began recommending both credit freezes and fraud alerts if you want true protection from unauthorized credit accounts. This is because credit bureaus are slowly removing some of the protections of the credit freeze due to widespread adoption and the elimination of fees. Basically, people are freezing their credit in record numbers, which is causing headaches to the credit industry.

All three major credit bureaus offer fraud alerts without any charge. However, choosing the best option is not always clear. Each bureau offers an initial 1-year alert, extended 7-year alert, or 1-year active duty military alert. My preference is always the extended 7-year option, but there are requirements to qualify. In order to obtain the 7-year protection, you must be the

victim of “fraud” and must submit proof of this claim. Traditionally, this would be a police report of identity theft. However, I am aware of many people who cited various popular data breaches and submitted letters of notification from the breached companies. If you possess a police report of identity theft, this is always preferred. If not, I believe you should attempt a fraud alert by providing whatever documentation you have which supports fraud potential toward your credit. Once you have identified the documentation you will be sending, navigate to the following websites and select the 7-year extended fraud alert.

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

<https://www.experian.com/fraud/center.html>

<https://www.transunion.com/fraud-alerts>

Follow the directions for each provider and wait for a mailed letter confirming activation of the alerts. Any time you seek a new line of credit, the credit bureau will apply more scrutiny toward your application, regardless of releasing a credit freeze. In early 2020, I applied for a new credit card as a test of my own security. The following details should explain why a fraud alert is necessary along with a credit freeze.

I have possessed a fraud alert through Equifax, Experian, and TransUnion since 2011. I renewed the alert in 2018. I always assumed it was unnecessary since I also possessed a credit freeze within all listed credit bureaus, but I like to push things whenever I can. I decided to apply for a new business credit card and knew the freeze would be a roadblock. I applied online for the card I wanted and expected a notice stating I had been declined, which happened right away. I was advised to place a call to customer support.

During the call, I was informed that my application had been declined due to the credit freeze. I intentionally applied with a freeze in place in order to test the security of the freeze itself. It passed the first test. The customer support employee told me I would need to release my freeze through Equifax in order to complete the application process. I played along, but also played dumb. I was directed to the Equifax credit freeze website which allowed an option to lift the freeze temporarily. However, I do not prefer this option during a credit card application.

Instead, I chose the option to grant a creditor a one-time code in order to access my credit report. This allows me to complete the application process without lifting the entire freeze for anyone else to abuse. It also prevents me from ensuring the re-freeze was properly executed. After selecting this option, I was presented a typical screen asking for personal details. I was also presented a field to enter my PIN assigned by Equifax during the credit freeze process. I was surprised to see an option to continue without providing a PIN.

While I knew my PIN, I selected the button that stated I did not know it. The customer support specialist confirmed that I would not need my PIN for this process. After providing my full name, physical address, DOB, and SSN, I was presented four “security questions” to verify my identity. These included selecting a known phone number, physical address, and previous employer from multiple choices. Afterward, I was presented a code to give to the credit card processor.

I want to pause here and vent my frustration. I placed a credit freeze in order to prevent anyone else from opening lines of credit in my name. I was mailed a PIN which would be required in order to lift the freeze. Instead, I was able to remove the freeze by supplying public information. My name, address, DOB, and SSN are available within numerous data breaches which are in the hands of criminals. The PIN was the only piece that was truly private, but it was bypassed by simply stating I did not possess it. The follow-up questions could have also been answered with publicly available data. The system is flawed. This is where a fraud alert can be beneficial.

After I gave the access code to the support representative, he was able to access my credit report. However, he could not complete the application due to my fraud alert with Equifax. This required him to verify additional information about me. He first asked me to identify the telephone number which I had attached to the fraud alert. I referenced my password manager which maintained these details and I provided the Google Voice number I had used during the fraud alert process. He confirmed it was correct. He then notified me that he would need to call me at that number.

We terminated the call, I logged in to my Yubikey-protected Google account, and answered the new incoming call to my “trusted” number. I again confirmed my name, address, DOB, and SSN over this new call, and the application was approved. Immediately after the call ended, I received a text message from a former colleague at the government building at which I previously worked. He told me that the credit card company had called asking for me, and thought I should know. Apparently, my old office number was also included on the “approved numbers” list.

I now believe that a credit freeze + fraud alert combination is the most protective solution in regard to preventing unauthorized access to your credit report. The freeze prevents a hard pull on your credit, but it can be defeated by a determined adversary. The fraud alert adds additional layers and should demand a phone call to a predetermined number. Possessing both should deter a common criminal looking for an easy score.

Verification Security Questions

You have likely telephoned a financial company in regard to your own accounts. Before a representative can participate in a conversation about your account, you must be verified as the account holder. This typically involves confirmation of a series of questions selected by you during account creation. The questions are selected from a small pool of options, and any honest answers are likely publicly available. As an example, one of the questions provided by my bank in order to secure my account is “What street did you grow up on?”. I am asked to answer this question honestly during account creation and I should be expected to answer this question whenever I call them.

This is an awful way to confirm a person’s identity. If I search for you within a free people search website, I will be presented all of your immediate family members. If I search for address history of your parents, I will see various home addresses which include date ranges of association with the home. After some simple math, I can determine the address of the home in which you were raised. Providing this detail could confirm me as you whenever I call to take over your account. Let’s fix this problem.

I previously explained how I use a software password manager to store my credentials. Whenever I create a new online account which requires answers to pre-selected security questions, I include these questions and answers within the notes area of each entry. I don’t have any preference of questions, as the answers I select will have nothing relevant to them. Let’s run through an example.

I created a new account with an online service. I had to select a security question, so I simply chose the first option which was “What is your favorite food?”. I opened my password manager (KeePassXC); made a new entry for this service; clicked the small dice icon next to the password field; and clicked the passphrase tab. This presented me with “stoneware thank” followed by many other words as part of a random passphrase. I supplied “stoneware thank” as my favorite food to the service. If I ever need to call support for this service and verify my identity, I will be asked for my favorite food, and my answer will be “stoneware thank”. If questioned further, I will explain that this is a delicious treat.

Please consider every important account which you have created over the past many years. Does your bank have security questions of which the answers can be easily found online? If so, please change all of them. I believe your security questions are as important as your passwords. If you plan to change your passwords to randomly-generated options, you may want to do the same with your security questions.

Plant Your Flag

I first heard the concept of planting your flag from journalist Brian Krebs. The idea is to identify common ways which criminals will try to infiltrate various online services pretending to be you, then take control of those accounts before a criminal does, even if you have no plans of using the online services. Consider the following.

Credit Bureaus: You likely already possess a credit freeze, but do you have actual online accounts with the major providers? These free accounts are practically worthless, but we don't want criminals to create them in our name. The following pages should allow you to generate online accounts and claim your profiles.

<https://my.equifax.com/consumer-registration/UCSC/#/personal-info>

<https://usa.experian.com/registration>

https://service.transunion.com/dss/orderStep1_form.page?

IRS: Tax fraud is a big problem. If you have an Identity Protection PIN issued by the IRS, your taxes cannot be filed without this private code. This eliminates most risk of fraudulent filings. The following website allows anyone to request a PIN, regardless of your status as an identity theft victim.

<https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>

If you want another layer of protection, consider creating an account with the Electronic Federal Tax Payment System at <https://www.eftps.gov/eftps/>. This is typically used by people who need to make quarterly estimated payments, but anyone can create an account (including a criminal portraying you).

Online Banking: Possessing a traditional checking account at your local bank may be enough to meet your financial needs. Even if you never plan to take advantage of online banking services, you should create an online account which is associated with your identity. You don't want a criminal to realize you have a bank account but no online login. This presents an opportunity for someone to access your account from anywhere in the world.

Cell Phone: Your cellular service provider likely offers an option to create a SIM PIN. In theory, this protects you from a SIM swapping attack. The protection is minimal, but there is no harm activating this feature. Contact your provider for details, but understand that it is not a bullet-proof mechanism. It is a small layer of protection, but there is no reason to avoid this strategy.

Voice Mail: Many people possess telephone voicemail without any type of PIN. These users simply call their own number from their device and immediately retrieve their messages. This creates the potential for a spoofed call which could also hear your voicemail. Adding a PIN to your account is an annoyance, as you must enter this code every time you collect messages. However, it prevents targeted voicemail attacks.

Utilities: You likely receive a paper bill from the power company every month. You can send a check or call and make a credit card payment. Almost every U.S. utility company offers an option to pay electronically online. Regardless of your desires to use this service, you should create the account in order to prevent someone else from claiming to be you. If your adversary knows your approximate location, asking to open an account in your name would likely disclose your home address. If you already possess an account, a second attempt would be refused.

USPS: Did you know that a complete stranger can receive scanned copies of every piece of mail you receive at your home? The USPS offers a service called Informed Delivery which is designed to notify you of pending mail being delivered to your home. Unfortunately, they require minimal information to verify authorization for these details. The following link allows you to activate this free service. Consider creating an account before your adversary pretends to be you.

<https://informeddelivery.usps.com/box/pages/intro/start.action>

State Unemployment Office: Unemployment fraud is a huge issue lately. Even if you have no plans to file a claim, consider creating an account with your state's unemployment office. This prevents a criminal from claiming to be you while requesting benefits.

DMV: While you may receive a postal notification of upcoming expiration of your driver's license or vehicle registration, online accounts can be created in your name quite easily. Consider claiming your online account and securing it with a strong password. This prevents the potential of unlawfully adding vehicles under your name and identifying your personal details provided to the state.

Insurance: Both home and vehicle insurance providers allow online accounts which display details of your coverage and allow digital payments. This is a potential vulnerability for high-risk targets. If I pretend to be you and create an account under your DOB, I can likely see your home address, vehicle information, and registration plate details. Protect this information by owning the online profiles which can access this data.

COVID-19 Concerns

I close this chapter with numerous privacy-related matters which have arisen during the COVID-19 crisis. Much of this book was written during the various stages of self-quarantine which was experienced by everyone throughout the world. While I selfishly benefited from the extra time which allowed early completion of this final draft, the pandemic introduced many new privacy concerns into all of our lives. This book will likely print before we see the end of these invasions, but I offer the following considerations for the next crisis.

Mobile Device Tracking

After most governments enacted rules which required people to stay at home unless travel was essential, we witnessed various levels of compliance. Some families practiced appropriate “social distancing” while others continued to attend large events. New cases of COVID-19 continued to emerge and many governments focused on technology as a possible solution. Many countries began tracking mobile devices in order to identify people who had possibly made contact with an infected person. The potential for abuse of this data is huge, so we should have an understanding of the technologies and threats.

Some countries relied on cellular connection details provided by mobile network providers. Cell phone tower logs can precisely identify the locations of devices (and people). This information can be used to detect large gatherings which violate local laws, or to identify devices which were within a few feet of a known infected person. Since most people purchase devices in their true names, it is easy to be identified as the owner of an account if you become a target. Some countries mandate that all device owners supply true information. In the U.S., we can easily mask our identity with prepaid plans, as previously explained.

Other countries have focused on application-based monitoring of COVID-19 infections. This requires effort by the end user while the previous cellular data monitoring is completely out of our control. I witnessed countries creating their own insecure apps which leaked potential sensitive data such as unique identifiers of hardware. In most scenarios, participation was voluntary. Some countries experienced a 20% adoption rate, but most needed at least 40% of the population to download the app in order for it to be effective. The typical goal with these apps is to identify people who may have come into contact with an infected person. If a participant is notified that he or she tested positive, this information can be reported through the app. The service then identifies devices which may have been in recent contact with the infected person and notifies them of the details. Typically, this occurs without disclosing any identities. However, apps created by government agencies usually are not very secure.

Finally, we have the execution of mobile device tracking by the U.S. government. Apple and Google partnered to create an infrastructure which could be used by third-party government

and private sector mobile applications. On the surface, this sounds incredibly invasive and undesired. You may be surprised to read that I welcome this partnership and execution. I will not pretend to understand all of the technical nuances presented by their teams, but I have great respect for their determination to never reveal any details which could be used to identify a person, device, network, or other unique identifier.

The product created by Apple and Google is not a tracking application ready for installation. It is simply a framework which can be used by other applications. It is embedded into the iOS and Android operating systems. The benefit with this is that it removes the necessity for governments to apply privacy-respecting methods while creating a tracking service. The framework will never disclose a telephone number, MAC address, IP address, name, home address, email account, or anything else which would identify the device owner to any application connected to the free tracking service. It assigns everyone rotating unique identifiers which are never associated with hardware or personal details. This way, government apps can receive data about locations of infections without knowing any true identities.

The purpose of this is to track movement of people and their proximity to others. When a person self-reports a COVID-19 infection through an app, it can notify others who may have been in contact with the infected person within the recent past. This happens behind the scenes without the ability to be abused. Have I drunk the Kool-Aid and installed any tracking apps? No. However, I embrace any attempt to properly mask identities of individuals versus hastily created apps by government contractors with no respect for privacy. This method is the least of all evils. Further, I encourage these actions in effort to eliminate any future deaths from this disease. As of now, all participation is voluntary.

I am updating this in 2021. I do not know how various final product(s) appear as you read this. Both iOS and Android operating systems currently have an option to disable any tracking, and all tracking is disabled by default. Hopefully, COVID-19 is now a distant memory. If we are still in this pandemic, we could experience mandatory usage of these technologies. In that case, we should understand our privacy options. First, possessing an anonymous device prevents much of any potential abuse. If an app collects your true cellular number, there is little to glean from it if you executed the strategies previously explained. Next, consider the location of the device. If a mandatory tracking app is present, then anyone with access to the logs would know the location of the device every night. You can defeat this with my Faraday bag methods as previously explained. Turning the device “off” is usually not enough.

It is easy for a privacy enthusiast to label all device tracking as invasive and unacceptable. I can relate to these feelings, but I also want to stay alive and healthy. Safety always trumps privacy for me. Personally, I would only participate within these programs if I were located in an urban environment with high risk of delivering or receiving the disease, and I believed that my usage would be helpful. You should make your own decisions without influence from me.

Working and Schooling from Home

During the pandemic, we all experienced a new way of life. Working remotely from home became a normal day for most people. While many embraced the idea of working in sweat pants, most ignored the privacy invasions which accompanied the transition. Employers began demanding that employees install remote conference software on their own equipment, most of which possessed some level of snooping software, and “always-on” webcams became normal. Working from home can be viewed as a luxury by some and a curse by others. The techniques within the previous chapters should minimize much of your exposure, but we should be aware of some common scenarios.

- Remote conference software, such as Zoom, collects and stores a lot of personal information during use. Be sure to always use a VPN, provide anonymous contact details, cover your camera when possible, and never install the software on your primary computer. Windows users might consider a dual-boot computer with a Linux partition for all work-related activities. Mac users could dual-boot two isolated versions of macOS on the same machine and boot into the work option during the day and personal at night. Overall, try to gain some isolation between your work device and personal data.
- Most conferencing services push users to download the official desktop software application in order to participate within meetings. This is usually unnecessary. Most meetings can be held within a web browser without any third-party download. Webex is one of the culprits. When you connect to a Webex session, their software is automatically prompted for download if you do not have it installed. If you simply cancel the download, Webex presents a link to “Join from your browser”. They hide this until you cancel the download, which I find inappropriate.
- Many schools demand installation of specific software which allows teachers to monitor students at all times. In most scenarios, instructors can watch students through webcams while taking tests or participating in lectures. This is a slippery slope toward abuse of the captured video or an eventual data leak. I encourage everyone to cover their webcams at all times in these scenarios. If you receive pressure from the school to enable a camera, explain that it appears broken and it does not work on any other apps. Again, never install proprietary remote conferencing software on any primary personal computer.
- If you would like to hear a full hour of my thoughts on working and schooling from home, please listen to my podcast devoted to the topic (163-Working & Schooling from Home). An online search of “zoom privacy dangers” should provide more reasons to protect yourself than you desire to read.

Vaccine Privacy Concerns

I am writing this section in April of 2021. I have numerous clients who have received the COVID-19 vaccine and each have experienced various levels of privacy intrusions. I suspect our society will face many future vaccinations for various viruses and variants, and booster shots will become a new normal. I present a summary of my findings for your consideration.

- Most states rely on some type of emergency and incident management software portal. These seem to vary by county and allow scheduling of vaccines according to tiers. Most of these demand a full name, DOB, postal code, email address, and cellular telephone number. All appear to accept masked email addresses and VOIP telephone numbers. Submitted data is typically not password protected, but a unique random URL is created for review at any time. These portals seem to be used for notification of eligibility and participation is not required to receive a vaccination. I avoid these.
- Each state possesses some type of scheduling portal. One popular example is PrepMod. This system allows individuals to register for an appointment and receive reminders of additional vaccinations. This system requests personal medical details, full name, DOB, full home address, and cellular number. It also accepts masked details and a PO Box. In order to access this data, an individual must know the unique URL and confirm a temporary code sent through email. You will likely be required to provide data into this system for a vaccine. The same system will be accessed during your vaccination and email updates will be sent to you through this network.
- Most vaccination clinics demanded photo identification during the visit. I believe this is mostly to confirm that the correct individual record was being updated. I am not aware of any clinics which attempted to scan any IDs into the system.
- None of the clinics demanded any proof of local residency.

Many clients asked if they should provide an alias name during this process. I strongly discourage this. Many of these clinics have a government connection and lying about your identity could be a crime. It could also prevent you from a future vaccination which could impact your health.

Overall, anticipate that any data provided could be abused. I do not believe patient data will ever be intentionally shared or sold, but I worry about breaches and leaks. Therefore, choose your data wisely. I instructed my clients to provide their true names and dates of birth. From there, anything else should be sanitized. VOIP numbers, forwarding email services, and mail drops all work fine. If this data is ever leaked, the damage is very minimal. If your burner email, VOIP number, and CMRA mail box become public information, it is not a huge deal. **Please make your choices about vaccinations based on your health needs and not paranoia.** If you choose to participate in this system, provide the best contact choices which you have available using the methods previously discussed.

The Next Pandemic

My concerns as I write this are not about the current pandemic. Today, we still have some control over participation in contact tracing and our data associated with vaccinations. By the time you read this, we may be under a full quarantine with mandatory access to our mobile devices. This would be quite difficult due to the privacy strategies available to us and the ability to simply conceal our devices in Faraday bags, but I never underestimate the capabilities of our government. I hope this book has provided the tools you need to take action which is appropriate for you, your family, and your desired level of privacy. Stay safe.

Summary

This is a large chapter which should be considered as a reactive response after you have established your desired level of privacy presented in the previous chapters. I typically advise my clients to consider the following after they are content with their privacy strategy.

- Identify home devices which require an internet connection.
- Eliminate network connectivity to these devices whenever possible.
- Consider data leakage from family and friends.
- Understand how disinformation strategies can assist those with unique names.
- Create proactive positive online content to help hide undesired search results.
- Create a personal website with a custom domain to possess desired disinformation.
- Monitor for potential adversaries attempting to identify home address.
- Remove undesired address and telephone data from the internet.
- Remove details from various mailing lists.
- Remove undesired online posts, photos, and videos.
- Establish a credit freeze, fraud alert, and credit opt-out.
- Change any accurate online security verification questions.
- Create accounts associated with your true identity when appropriate (plant your flag).
- Apply proper privacy and security protocols while working remotely.

CHAPTER SIXTEEN

PHYSICAL PRIVACY & SECURITY

In 2017, I co-authored a book about physical privacy and security considerations as part of the Complete Privacy & Security Desk Reference series. Both volumes of the series are now out of print and severely outdated, but there were many timeless strategies which can benefit us privacy enthusiasts. My attempt in this chapter is to briefly summarize the content of that book, which is not otherwise present in this edition, in a way which can be easily digested. I present a lot of content here, compressed into glossary-style text, which can be further researched if desired. My goal is to get you thinking about these considerations as you establish your new private life. Let's begin with protecting the physical privacy of your home.

Home Privacy

After you have spent so much effort moving into your new anonymous home, you should execute best practices in regard to your physical privacy. Titling your home to the name of a trust loses privacy protection if your trash contains personal mail; legal paperwork can be seen through windows; and your business cards are visible within your vehicle parked in the driveway. The following tactics should be considered at all times.

Park vehicles in garage: There are many opinions on this. Some believe leaving a vehicle outside the house may convince a would-be burglar to stay away since someone is likely home. However, you obtain a potential layer of security at the risk of losing privacy. An exposed vehicle displays a license plate which can be swept into various license plate recognition systems. It is also prone to vehicle burglary and displays a pattern of behavior. If the vehicle is always present, but then disappears one night, you may be inviting unwanted trouble while you are gone. My strong preference is to always park any vehicles in a garage without windows. This allows you to conceal vehicle identifiers, items being transported into and out of the vehicle, and creates an overall assumption that someone COULD be home.

Properly eliminate personal trash: In the United States, I am legally allowed to take possession of any trash in front of your home. I can "steal" all of the bags and analyze them later when convenient for me. In fact, I did this during numerous investigations when I was assigned to a drug task force in the late nineties. During one assignment, we were preparing to execute a search warrant at a home later in the week on an early Friday morning. A call to the local trash service confirmed that Thursday was "trash day". On Wednesday night, I drove

by the target location and observed several full trash bags within the designated pickup container. I grabbed them all and threw them in the trunk of my covert police vehicle. At the police department, I opened the bags and located paperwork confirming the main suspect resided at the home; receipts disclosing bulk purchases of drug-making supplies; and empty boxes of 9mm ammunition.

While this evidence was circumstantial, the discarded ledger of completed and pending drug sales provided an interesting piece of testimony at the trial. You could have replicated my actions without any legal repercussions. While my clients are not hiding from drug-related search warrants, they do have concerns about stalkers, former lovers, and paparazzi. The following trash protocol is taught to anyone hiring me for a complete privacy reboot.

Isolate any trash or recycling which contains true identities. This can include mail brought into the home after delivery to a UPS store, unwanted documents, private photos, expired credit cards, or any other sensitive items. The rule is that there should never be any evidence of a person's true name or image in the trash or recycling containers. Often, I will remove any labels from shipments I have brought into my home which contain my name. I can recycle or discard the package material, but never the labels.

Anything with a true name gets shredded into a cross-cut shredder. I currently use the AmazonBasics 6-Sheet High-Security Micro-Cut Paper and Credit Card Home Office Shredder (amzn.to/2SGjDQq). This device shreds paper into 5/32" by 15/32" pieces. While this is a strong start, some text can still be read within the pieces. Once weekly, I burn all shredded material in a designated container outside my home. The combination of these two techniques ensures evidence of my identity is not available in my trash.

Apply proper window treatments: The term "proper" is quite subjective here, but I offer my guidance to clients. Any windows displaying access to the garage should be covered at all times with a material which prevents any view. I prefer to apply frosted glass spray paint to the interior of all garage windows. This allows light to enter without exposing clear details and eliminates accidental movement of curtains or blinds which could allow viewing from the outside.

I also try to identify the most common windows which will be viewed from a potential intruder. These are often the windows by the front and rear entry doors. Any window with easy access from a visitor should be covered with a curtain or blinds at all times. On occasion, walk the perimeter of your home in the way a potential intruder would investigate the premises. Identify any likely areas which could help determine that no one was home. Overall, you want privacy within living areas without the appearance of being a shut-in.

Eliminate personality from the exterior of the home: Before writing this chapter, I took a walk around my neighborhood. One home proudly displayed their child's high school football player number, which also identified the grade and school. I now know they have a high school senior named Tim who wears number 21. The house next to them displayed a large wood sign proclaiming the "Wilsons" to possess the home. Next to them, a neighbor possessed a sign announcing their love for Scottish terriers and a doghouse identified as the home of "Max" and "Greta". One of my neighbors spray-painted his last name on his trash bin, and displays a notice in his yard about his wood-cutting services. All of these scenarios present enough vulnerabilities to initiate a believable social engineering attack. While highly unlikely, these details could be abused. I prefer my clients to display no signs of interest or names.

Eliminate personality from the interior of the home: This one may lose several readers. If you are in the need of extreme privacy, you should eliminate all items within your home which might disclose your name or immediate family members in view of guests. Consider a few examples.

Wall of Fame: Most of us, including myself many years ago, possess an office or other room which proudly displays our achievements. In 2010, my home office displayed numerous awards on the walls. When a Charter internet technician came to troubleshoot a dying modem, a quick glance at my wall launched an uncomfortable conversation about my work. I no longer display any awards and I encourage many clients to do the same.

Personalized Gifts: Many gifts include some type of personalization such as engraving or printing of a family name. If you have your true name engraved on a door knocker, but you have convinced your neighbors that your last name is something else, this could cause unwanted inquisition. If your wedding album, with a custom cover announcing the true names and date, is visible on the coffee table, it may generate questions which you do not want to answer. After a client with an extreme situation moves into a new anonymous home, I conduct a sweep, attempting to identify any items which may need to be hidden. This can also include trophies, crafts, blankets, and collectibles which are too revealing.

Family Keepsakes: This one is the most difficult. Many of us possess items which have been handed down through several generations. Old newspaper articles, historic photos, family recipe books, and anything else which displays a family name can be trouble. These items should be carefully stored out of public view. I have witnessed stalkers and ex-lovers sneak around a suspected new home of their target in order to confirm their suspicions. The presence of one item containing the victim's name could be enough to cause someone to take their obsessions further.

Home Security

While you may be anonymous, you are not invisible. Criminals may not care about your identity, but are happy to take advantage of a vulnerable home in order to steal your items. While not directly related to privacy, protecting your family and valuables from crimes of opportunity makes good sense. If you need an extreme privacy example, consider the repercussions of a crime being committed at your home. A publicly-available police report displaying your true name and address associated with a burglary can eliminate all privacy strategies in place up to this point. Therefore, it is in your best interest to protect your property from potential crimes and the need to involve law enforcement. I present several ideas, beginning inside the home followed by exterior considerations.

Keep your valuables out of sight: This one may seem fairly obvious, but most people ignore the recommendation. Jewelry boxes on top of dressers, rare firearms behind hanging glass frames, and expensive laptops on the kitchen counter are all enticing to a burglar. A home free of visible items which can be quickly sold or traded may be passed for a more lucrative option.

Hide small valuables in unique places: Most thieves want something small and valuable. Money, jewelry, prescription drugs, and collectibles can be removed from a home quickly, and hidden within pockets while walking down the road. Because of this, I recommend placing small valuables within items which would likely be ignored during a burglary. First, I want to discuss popular options which I think are awful ideas. I NEVER recommend the following.

- Hollow books: Many burglars will quickly analyze books on a shelf knowing that empty decoys are commonly used to store valuables. It does not take long to identify the overly thick book with little weight.
- Anything in bedroom: Most thieves go straight to the master bedroom in order to find valuable loot. This is likely the worst place to keep anything important.
- Freezer/Refrigerator: This has become one of the most popular places to hide valuables, and thieves have been paying attention. It is fairly easy to identify items in a freezer which appear out of place, and this should be avoided.

This leaves us with the following options which are more ideal.

- Trophies: Almost all trophies are hollow within the metallic-coated pieces. Unscrewing these and placing small valuables inside are likely to go undetected. Placing all of the trophies in a cardboard box in the garage will add even less interest. If you possessed my sporting ability growing up, you can buy your own trophies. I once visited a trophy store and asked if I could buy any defected items. I walked out with a box full of awards I could never earn at a cost of \$10. These could be used to hide thousands of dollars.

- CD Player: I recall the days when a full-sized CD player within a stereo cabinet would be a prime target for a theft. Today, they are ignored and practically worthless. These oversized electronics consist mostly of open air. Removing a few screws on the back reveals an opportunity to store small and midsized valuables. Cassette decks are also great for this.
- Electrical outlet: As mentioned in a previous chapter, I prefer electrical outlets as hiding places for extremely small items. There is usually a small amount of space surrounding the outlet itself, and commonly a hollow wall nearby. I have never known a burglar to remove outlet faceplates to take a peek behind them.
- Novelty hiding devices: Be careful here, but you can find many common household devices which have been converted into empty hiding places on Amazon.

Present “bait” to any burglars: Some physical security professionals laugh at me when I mention this, but I stand by my recommendation. I believe every home should have items which solely serve as bait to a would-be criminal. My favorite consideration is the small fire safe filled with heavy objects. I keep two Sentry fireproof boxes (amzn.to/2HPfyD2) in my home at all times. One is under my bed and the other is in my bedroom closet. Each are filled with four 5-pound plates taken from a set of old dumbbell exercise weights, a few rolls of pennies, and some loose change. They are locked with no keys in sight. When a burglar looks in these two places, which is extremely common for a thief, the safes will rattle and be heavy. Most will assume that a firearm or bullion is inside, and these two items will be top priority for taking.

This serves a few purposes. First, it wastes the energy and time of the burglar. Hauling out two 20-pound boxes is plausible, but not fun. Since most burglars do not bring a vehicle to the scene of the crime, he or she must carry this weight some distance. For bonus points, remove the plastic handles from the boxes to make carrying more difficult. If desired, a larger safe could be used with more weight. Next, this tactic may prevent a burglar from taking something more valuable. If he or she believes that a prize is already in hand, a second trip back may be viewed as an unnecessary risk. Finally, it serves as a clear indicator that a crime occurred. Many burglars enter and retreat undetected. They leave no sign of foul play until you discover the theft weeks later. This presents a good chance of avoiding capture. If you see that one of these boxes is missing, you know something happened.

Install a large safe: This is mandatory for any home in which I live. A large stand-up gun safe can hold a number of valuable items and can be made very difficult to move. They are never completely burglar-proof, but we can take actions to make them extremely difficult to compromise. First, only consider safes which have the option to be bolted into a floor. There are many installation variables, but the idea is that you bolt the safe from the interior into the flooring below. Ideally, this would be a concrete surface, but bolting into a wood floor is also an option. Proper safe installation is outside the scope of this book, but free information is

plentiful online. While I demand my safe to be bolted into a floor within the interior of my home for easy access, I respect this is not always an option. Therefore, I offer a few suggestions for placement and weight which may burden a thief enough to move onto something else.

First, consider the location of the safe. I see many people place them in garages due to size and weight, but I do not approve of this. If it was easy to move into the garage, it will be just as easy to move out. I want to make it a struggle for the thief. I also want the safe within the home in case I need to access it quickly. If you keep your firearms in a safe due to the presence of children, you should be able to easily access them within your home in the case of an emergency, such as a home invasion.

For most clients, a large gun safe is placed in the basement. If the basement does not have an exterior door, this makes the safe especially difficult to remove. Carrying an empty 400-pound safe up the stairs is quite a challenge. Fill it with heavy items and you have a bigger problem. I have also placed safes behind false walls, but this usually requires carpentry abilities. Recently, I placed a safe within a closet in which the safe was wider than the closet doorway. Removing the trim and door allowed just enough room to squeeze it in. Securely replacing the trim and door created a scenario where the safe could not be slid out of the closet without repeating the process. Numerous three-inch screws through the solid wood trim into wall studs creates a frustrating experience for a burglar looking to escape quickly.

Many gun safes possess various gun racks in order to vertically store long guns. I usually remove these in order to possess an open box. On a few occasions, I have added custom shelving or premade short book cases from Ikea in order to take advantage of the space. My next goal is to make the safe as heavy as possible without exceeding an appropriate weight for the flooring. If within a basement with a concrete floor, I see no limitations. The heavier the safe, the less likely a burglar will try to remove it. I have used the following techniques on behalf of clients.

- Ammunition: I admit I am a bit of an ammunition hoarder. I am not a doomsday prepper, but I believe every gun owner should have more ammunition than they think they might need. My home safe contains over 100 pounds of ammunition which makes it extremely difficult to move.
- Bullion: I had a client who collected 10-ounce silver bullion bars. He believed this was a protection from a collapsing dollar, and had boxes of it. Lining the bottom of his safe with these bars added over 150 pounds of weight.
- Worthless Materials: If you simply want to add as much weight as possible to your safe, you can find numerous options at your local home improvement store. 50-pound bags of sand are less than \$5.

If you possess a gun safe which only contains a few guns and a small amount of ammunition, two people can easily carry it out of your home. A 400-pound safe which contains 400 pounds of content creates a surprise for a criminal duo. While not impossible to remove, it will be very difficult and take some valuable time. Consider the desired content and location of your safe before purchase. Once in place, consider storing any valuables within it and have some piece of mind while away from the house.

Utilize lamp timers: A home which is dark for 24 hours is probably empty. If it is dark for a few days, the residents are likely out of town. Placing an interior light on a timer can give the impression that someone is home. However, creating a pattern of specific times during which it is turned on and off can create an illusion of automation. Because of this, I prefer programmable timers which can be staggered. I currently recommend the BN-LINK 7 Day Digital Programmable Timer (amzn.to/2HLTgCc). It allows programming of two lamps at different times over multiple days. It also has a vacation mode which randomizes the times in which lamps are activated. Always test your settings before execution.

Consider fake television visuals: Many people leave lights on when they leave the home. This does not deter many desperate burglars. However, evidence of a television being watched is usually a sign that someone is home. A television left on constantly while you are away can be harmful to the device and a sign that this is a ruse to deter burglars. This is where I recommend a “Fake TV”. This small device emits random lights which simulate the look of a television being used in a dark room. An example for less than \$20 which I have used can be found at amzn.to/2vYalGx. Adding this product to a lamp timer can create a desired effect which can fool many into believing someone is home.

Consider audio applications: If you do not want to invest in timers and visual decoys, a simple AM radio can accomplish a lot. Pick a talk station, increase the volume enough in which it can be heard from every room, and leave. If a burglar enters, the audio may be enough to make him choose another home.

Install exterior lighting: Exterior motion lights are more affordable and brighter than ever before. If you do not have existing lights pre-wired and do not want to risk shocking yourself during installation, battery-powered and solar options are plentiful. Most burglars will move on if lights activate when they get near a home. This is a small sign that the homeowner takes security seriously and that there are likely additional security measures in place inside the home. This is a small layer of protection, but I see no reason to ignore this strategy.

Activate an alarm system: Alarms can be quite a deterrent. They can also be a huge privacy invasion, which I explain at the end of this section. First, let's focus on the benefits. If a burglar enters a home and triggers an audible alarm, he knows his time just became much more

limited. He does not know if you subscribe to an alarm service which has just notified the police. A nosy neighbor may hear the audible alarm and choose to investigate.

Either way, you are no longer an easy target and there is added pressure for him to leave quickly. Audible alarms wirelessly connected to sensors on doors and windows are plentiful. All have security weaknesses and are targeted toward the local amateur burglar. A sophisticated adversary will know ways to defeat standard protection, but that threat is fairly rare, especially if you are not a heavily targeted individual.

I do not typically recommend any type of monitored alarm systems. I have many clients in Los Angeles who insist on this, and private security vehicles continuously respond to alarm activations day and night. My concern is due to false alarms which trigger a police response. Imagine you are in your anonymous home without any association to your true name. While working in the garage, your alarm malfunctions or is accidentally triggered. Your alarm company cannot reach you by phone to confirm everything is fine and dispatches the local police to check on things. An officer pulls up and determines you likely belong to the home. You will be asked to provide identification, and your name will forever be connected to your home within a police report. I simply cannot risk this for myself or my clients. I encourage them to stick with audible alarms which are not monitored by any outside agency.

Display signage of protection: Whether you possess a functioning alarm or simply want to convey that you do, alarm signage is an affordable and effective solution. Small alarm notification stickers strategically placed on doors and windows likely to be used for illegal entry may deter a random thief. Signs near the driveway and home announcing the use of an alarm system can also be helpful. Both Amazon and your local hardware store offer many options.

Replace locks, strike plates, and screws: This is another mandatory action taken on any home for myself or a client. Changing the locks is standard practice when moving into a new home. If renting, you may receive resistance from a landlord over this, but I believe the battle is worth the reward. If you can afford expensive locks such as those made by Medeco or Abloy, that is great. However, most of my clients simply do not want to spend over \$200 on each door. Instead, I encourage them to look for the grade of the lock. Grade 1 is the highest rating a consumer lock can receive. Grade 1 deadbolts were once primarily limited to industrial buildings but are now abundant for residential use. However, the grade of the lock will become useless if you do not reinforce your strike plates.

A typical lock strike plate is a small piece of metal within the door frame. It is the “hole” in which the locking mechanism secures into the frame of the door. These are usually secured with two short screws and can be compromised easily with a swift kick to the door. Because of this, I highly recommend two strategies to better secure your exterior doors. First, replace the strike plate with a larger version requiring four screws (amzn.to/2VcIjS9). This may

require you to modify the frame by chipping away room for the plate. Next, secure the plate with three-inch screws. This ensures that the plate is securely connected to the studs of the wall and make forced entry much more difficult.

Remove external keys: We have all seen a TV show or movie in which a person visits the home of a family member or friend and finds the front door to be locked. After a quick look around, the person picks up a false rock or finds a hidden box which contains a backup key. Those days of innocence are over. Every burglar knows to look for a hidden key near the door and can spot a fake rock quicker than you or me. My stance is firm. Never place a backup key anywhere exterior to the home.

Install a fence for security (not privacy): Six-foot privacy fences are appealing. They prevent street traffic from seeing into your home and isolate you from the nosy neighbors sitting in their yards. However, this comes at a price. The same fence which prevents visibility into your home provides concealment for anyone committing crimes on your property. A steel security fence is ideal for those wanting to keep people off of their property while a solid privacy fence is appropriate for those wanting visual isolation. I am “on the fence” a bit on these. Identify your own priorities and proceed accordingly.

Secure utility boxes: Many homes possess a utility panel outside the home which is maintained by the power company. This could be on an exterior wall of the home or attached to a pole near the street. When open, it usually presents a single master switch which disconnects the power to the entire home. If you possess a box like this, please consider securing it with a high-security padlock. This will not prevent a prepared thief who brings bolt cutters, but it may thwart a burglar looking for any easy opportunity.

Modify patterns of behavior: The final recommendation to is to change things up. If you leave at the same time every morning and return at the same time every afternoon, you set a pattern of behavior which can be abused. While you may not be able to control departure times due to a rigid work schedule, there are other things you can do. Returning home during lunch on occasion may break up a routine being monitored by a criminal neighbor.

Misleading Props: Randomly leaving dirty work boots outside a front door may convince a passerby to move on. Even without a pet, a large dog food bowl and half-full water bowl near the door may be enough to convince a thief to move on. Combining this with a thick rope attached to the deck may create the appearance of a brutal guard dog within the home. Get creative.

Travel Security

I have traveled extensively and experienced pick-pocketing, hotel room theft, and even an unfortunate physical attack. Criminals prey on visitors unfamiliar with their current environment. The following are some basic guidelines I follow any time I am on the move.

Empty Pockets: I never keep anything in the pockets of my pants, jacket, or other clothing. Bulging pockets are a common target for thieves. We all think we would notice someone entering our pockets, but I can tell you from experience this is not the case. While traveling, all vital items are stored in my backpack.

Secure Bag: Whether you prefer a backpack, messenger bag, or other type of satchel, keeping belongings in a properly secured bag typically provides more protection than pockets. I am less likely to lose an item if everything is in one bag while navigating airport security than if I have a wallet in one clothing pocket and a phone in another. Empty pockets allow you to focus on a single collection resource and prevent the “pat all the pockets and see if I forgot anything” dance we see after a security inspection. I prefer bags which possess numerous interior pockets, each with their own zipper. This requires more effort by thieves to steal your goods. I also prefer to lock the zippers of all exterior pockets. I make the two zipper pull tabs meet and lock them together. If it is a pocket which I do not need to access during travel, I may use a zip tie and cut it later. If I need access the pocket during travel, I may use a strong wire twist tie, Velcro cable strap, or even a small padlock. None of these prevent forced access, but each should provide an obvious alert that an entry attempt was being made while the bag was on your back or shoulder.

Always In-Sight: My bag is always on my person and never out of sight. If I remove any content, it goes straight back in immediately after use. In the hotel room, I never use any drawers or storage compartments. My bag stays packed at all times, ready for a quick departure if needed. This eliminates much risk of accidental loss or theft. When I leave the room, my bag goes with me. Hotel safes are not secure and should be avoided.

Demeanor: Always blend in as much as possible, especially in your dress and appearance. Don’t have an appearance as a tourist, such as wearing a t-shirt from the local gift shop. Never view maps in plain view; always prepare for your journey in the hotel room.

Secure Room: Always lock your hotel room the best as possible. When inside the room, take advantage of all locking mechanisms on all doors, connecting rooms, and windows.

Copies: I recommend possessing digital copies of all important documentation, such as your license, passport, and credit cards. This can be very helpful in the event of stolen or missing items. I keep my files on an encrypted micro SD card sewn within a pocket in my pants.

Faraday Wallets

I previously explained my use of Faraday bags with mobile devices in order to prevent signals from being sent to or from my phone. I apply this same strategy to my wallets in order to prevent electronic chips embedded into my credit cards from being maliciously compromised. My three main concerns with credit cards are magnetic swipes, physical EMV cloning, and wireless RFID capture. Let's understand each.

The magnetic strip on the back of most credit cards contains static data. Any magnetic reader could collect the customer's name, credit card number, expiration, and card issuer details. The security code printed on the back of the card is not included in this data. Criminals with card "skimmers" are eager to get their hands on your cards.

EMV, an acronym for Europay, Mastercard and Visa, is a global standard for credit cards equipped with computer chips and the technology used to authenticate secure transactions. Many U.S. card issuers have migrated to this new technology to protect consumers and reduce the costs of fraud. Unlike magnetic-stripe cards, every time an EMV card is used for a payment, the card chip creates a unique transaction code that cannot be used again. If a criminal stole the chip information from one specific point of sale, card duplication would never work because the stolen transaction number created in that instance would be declined. EMV requires direct contact, and wireless capture is not (currently) possible.

An RFID credit card is a contactless card which interacts with a card reader over a short range using Radio Frequency Identification (RFID) technology. RFID-enabled credit cards, which may also be advertised as "tap to pay" cards, have tiny RFID chips inside the card which allow the transmission of information. The RFID chip itself is not powered, but instead relies on the energy transferred by an RF-capable payment terminal. The range of RFID in this scenario is typically under three feet. Numerous security professionals have demonstrated various abilities to acquire RFID data from credit cards remotely. Discovered vulnerabilities within the encryption protocols are quickly patched, but this is always a game of cat-and-mouse.

While magnetic stripes and EMV chips are not a threat from wireless capture devices, RFID cloning has been proven possible. Because of this, I place all cards inside a Faraday wallet. I currently use the Silent Pocket Slim Wallet (amzn.to/3tmB7kl). I have different colors for each of my alias wallets, as previously explained. These wallets block all wireless signals, including RFID. This allows me to protect any credit cards, licenses, passport cards, or other cards which may possess this technology.

Firearms

I am an advocate for gun ownership and concealed carry of firearms. I rarely leave my home without a firearm properly concealed and accessible. This is not a book about firearm safety, training, or concealment practices. Instead, I want to focus on a scenario which has presented problems to privacy enthusiasts. Every state in the country possesses unique laws about gun ownership, purchase, and carry. South Dakota has its own nuances.

If your domicile is South Dakota and you possess a PMB address on your driver's license, you can legally purchase a firearm while you are inside the state boundaries without a permit. If the seller possesses a Federal Firearms License (FFL), he or she will likely execute a background check through the National Instant Criminal Background Check System (NICS). This usually results in a 48-hour hold on the sale. However, this is not required by state law and a private seller may not conduct a check. Overall, buying a gun within the state is fairly easy and straightforward. There is no official waiting period and weapons do not need to be registered with the state. While in the state, you can legally carry an unloaded handgun in the trunk or other closed compartment of a vehicle without any type of permit. Open carry is legal in South Dakota, which means you can carry a loaded weapon on your person without a permit, as long as it is visible to the public. Carrying a concealed weapon, especially in other states, is where it gets tricky. South Dakota offers three levels of concealed carry license, and I will only focus on the "Enhanced" option which allows concealed carry in 37 additional states. The enhanced license requires fingerprinting, a federal background check, and a firearms safety course. It provides the most features in terms of reciprocities with other states. However, there is a catch.

South Dakota requires that the applicant has "physically resided in and is a resident of the county where the application is being made for at least thirty days immediately preceding the date of the application". By the letter of the law, you must be physically present within the state for a month before you apply. This could be a hotel or RV park with a physical address. I have spoken with numerous Sheriff's deputies about this. Half insist on the physical presence while the other half stated that the PMB address is sufficient. If this is your scenario, I encourage you to do your own homework and contact the Sheriff's department within the county of your domicile. You can find complete current instructions for concealed carry permits on the South Dakota website at <https://sdsos.gov/general-services/concealed-pistol-permits/default.aspx>. Overall, I encourage potential South Dakota nomads to consider their firearm and concealed licensing needs when they conduct the rest of their transition to the state. If you are not a South Dakota nomad, you are at the mercy of the laws of your state. I recommend visiting <https://gunstocarry.com/ccw-reciprocity-map> for more information. Being a nomad will always have potential negative implications in your legal ability to carry a firearm. I encourage you to keep advised of any changes in the laws of your state.

Dealing with Drones

Assume you have established your perfect anonymous home which has no association to your real identity. You chose appropriate window treatments and made sure you have physical privacy from the street. You then hear the buzzing of a drone right above your house. What can you do? Some will say you can shoot it down, but in most states you legally cannot. Some believe it is illegal to fly a drone over another person's property, but it is usually not.

These annoying flying devices are a huge privacy invasion, as almost all of them record and transmit high-definition video, but there are few legal protections which allow us to take action once they appear over our property. None of the following should be taken as legal advice. I simply present some personal thoughts on dealing with drones. More information can be heard on episode 194 of my podcast.

- Never shoot a gun toward a drone. Bullets must land somewhere and we do not want innocent bystanders getting hurt. Some states classify shooting at a drone as the same crime as shooting at an occupied aircraft.
- If a drone is flying close to you or your home, a high-powered water hose or pressure washer can cause the unit to crash. If the unit lands on your property, you do not have a legal right to take control of it, but a No Trespassing sign prevents the owner from legally retrieving it.
- Small projectiles such as paintballs and BB guns are not very effective at knocking the devices down. However, a well-aimed football can cause a crash quickly.
- Signal jammers rarely work and are usually considered illegal. Most drones have a feature which sends it back to the original departure GPS location if it loses signal.
- Some people buy their own drones to fly into invasive drones floating over your own property. This may destroy both devices.
- Some companies are creating drone-catching nets which can be launched on your own property. This seems excessive to me, but may be a last resort for you.
- U.S. federal law requires all drone owners to register their devices and display the registration number on the unit. However, almost no one does this. You can report your neighbor for violating this law, but do not expect much enforcement.
- Calling the police about drones will rarely result in any enforcement. Some states such as Arizona, Arkansas, California, Florida, Kansas, and Louisiana have laws targeted toward improper drone usage. However, involving the police will result in a requirement to disclose your true identity and location. Police reports are often considered public information. Decide if your potential loss of privacy justifies your desire for revenge.
- You have no right to privacy from drones flying within public spaces. Be cautious.

Summary

Physical safety is more important than any privacy strategy. Every client who desires a new anonymous home for privacy reasons receives the following summary list for physical security considerations.

- Vehicles should be parked in an attached garage with no clear windows.
- Never discard trash with items in your true name.
- Shred all sensitive documents.
- Apply proper windows treatments throughout the home.
- Consider removing personality elements from the exterior and interior of the home.
- Keep all valuables out of sight from the exterior.
- Properly hide small valuables within the home.
- Consider “Bait Safes” to attract burglars.
- Properly install a large safe for firearms and valuables.
- Properly utilize lamp timers, radios, and artificial TV lights.
- Install exterior lighting with motion sensors.
- Consider benefits and risks of alarm systems and signs.
- Replace all locks and add new strike plates and long screws.
- Consider fencing benefits and risks.
- Modify patterns of behavior to mask obvious schedules.

CHAPTER SEVENTEEN

MY SUCCESSES AND FAILURES: JANE DOE

I wish I could tell you this life has been easy. I wish I had a guide for all of this while I was experimenting. I have been forced to test new strategies on myself, and occasionally clients. I have made my share of mistakes, and I have learned valuable lessons from each. These next few chapters serve as final tales of my various successes and failures when trying to make people disappear. I hope that these true stories provide insight which will aid the creation of your own privacy strategies, and give you a final confidence boost to achieve any level of privacy you desire. Obviously, all of the people mentioned have given consent to share these stories. I have redacted and modified many details to protect their identities. First, we meet Jane Doe.

I received an email through my website from a man that only asked if he could speak to me over the telephone about a sensitive situation. The name he used was the same as a fairly wealthy individual who served as an initial investor in a few successful businesses. His area code matched the general location of the investor, and his email address had a domain associated with a company that was registered to him. I scheduled a call for the next day. Those who have read my other books will know that I take every layer of my privacy very seriously. I would never call anyone from my actual cellular telephone number, and I try to avoid using Google Voice for anything too sensitive. Google keeps a log of all incoming and outgoing calls forever, regardless if the history was deleted by both parties. I also never call a cellular number of a potential client. I have no way of knowing whether the person's phone possesses malware that records calls and text messages, forwarding them to the adversary. The metadata of all calls and messages is stored by the service provider and a subpoena could make record of our communication admissible in a civil court. Instead, I instructed him to use the application Wire, which was discussed previously in this book.

I asked him to install Wire to a computer which he was confident had not been compromised, and not a mobile device. He would need to create an account and email me the username chosen. I would then call him through this app at a specified time for an audio call. While video calling is supported, I have no idea of what I am getting myself into. I don't want a stranger to save a screen capture of my face and later post it on the internet. I know that sounds a bit paranoid, but it is better to be safe than sorry.

We connected on Wire and made brief introductions. He was a savvy business person that knew how to get directly to the point. He stated that his daughter was in a true mess and he had no idea what to do. She had recently terminated a long-term relationship with an abusive man. The former companion was extremely upset and unstable. He confronted her at a friend's home where she had been staying and attempted to abduct her. She fought and was injured slightly during the process. She has always turned to alcohol and drugs to fight stress and was in a rut dealing with a boyfriend turned stalker. No matter where she stayed, he knew where she was. When she went out, he was there soon after. He even approached her in a grocery store demanding that she take him back before he "really" hurts her. She felt her world was out of control.

I asked the potential new client what level of help he was seeking. He immediately responded "the full treatment" and asked how quickly I could help. He wanted me to relocate her to a safe place where the boyfriend could never find her. He did not care about the cost, and assured me he would pay any expenses. We set up the details of establishing a retainer that would allow me to start getting things in place. While he was funding this adventure, I did not consider him to be the client. I advised that I needed to speak with her directly to start a plan and identify how exposed she was. He agreed to allow her to use his Wire account from his device and we arranged a call for the next day. Before we terminated the secure communication, I asked for the name of the boyfriend and as much detail about his life that could be provided. He only knew a name and occupation, which was plenty to start my own stalking.

"Chris" was a 30-something computer systems administrator who appeared tech-savvy. His Facebook and Instagram pages were decorated with photos of network cabling installations. This is often referred to as "cable porn", and high-tech people are fascinated by routers and switches which possess perfectly installed network cabling, often hundreds of strands of wires. He had a GitHub page which tells me he understands technology more than the average stalker. This was most concerning as it often means that malicious software was installed on the victim's devices.

I was glad that we would be communicating on her father's computer. Chris had a cellular telephone number associated with his Facebook account, and a password recovery attempt identified the last two digits of the number. A search of his Instagram username on the website FindMySnap.com, which is now retired, revealed that a SnapChat username existed identical to the Instagram account. Furthermore, this SnapChat name had been in existence since prior to 2013 when a data breach leaked user information to the internet. This revealed the first eight digits of his cellular number. Combining the SnapChat and Facebook results revealed a potential entire cell number. Placing this number with country code into the Facebook Messenger app confirmed that the number was connected to his profile. This confirmation allowed me to further investigate his online presence.

I created a virtual Android phone using software called Genymotion which allowed me to use mobile apps on my computer. I placed his cellular number in my contacts phonebook within Android and left the name as Chris. I then installed several popular social networking applications on the device and executed the “Find My Friends” feature on each. This revealed the networks where he has profiles as most require a cellular number to establish the new account. I now had a good understanding of his online activity which would later prove to be valuable.

During my call with Jane, she seemed extremely scared. She said that he will never give up and that I was probably wasting my time. She knew he would find her and continue to harass her no matter where she went. She had given up on me before I could explain my process. I asked her what type of phone she had and where she got it. She stated that she had a Samsung Galaxy S6 and it was given to her by her former boyfriend. She confirmed that there were no Samsung stock apps anywhere, which convinced me that he had “rooted” the device. I had a strong suspicion that he had installed malicious software (malware) on her phone which was allowing him to see her location at all times. He could likely monitor her communications which would identify the friends with whom she had been staying. I advised her to keep the phone on, and send it to me via overnight Fed-Ex at the hotel where I was staying. I told her to go to an Apple Store, with her dad, and pay cash for a new iPhone of her choice. After purchase, I instructed her not to open it and call me on Wire from her dad’s computer when ready to turn it on for the first time. She agreed.

While waiting to analyze Jane’s phone and talk with her on a secure line, I decided to also dig into her life a bit. Similar to how I investigate the offenders of the situations with which I assist, I also conduct a thorough review of the victims. Early in my new privacy career, I was approached by a woman in her twenties requesting help hiding from her abuser. “Martha” explained how he was mentally and physically abusive to her and their young child. She did not feel safe and knew he would try to track them down wherever they went. I was eager to protect her from a future attack.

I began planning her move and made sure that there would be no trail that he could follow. I assumed that only women could be victims in these types of scenarios. It never occurred to me that she might be the problem in the relationship. Fortunately (and accidentally), I found an old Facebook post made by the father of the child. It displayed a screen capture of a court order allowing him full custody of the child. I could not see the details of the order, but the father was very excited that this day had come. I finally located the full court order which detailed the mother’s drug abuse, child neglect, and three documented occasions where Martha tried to abduct the child and leave the country. This led me to court documentation about her mental issues and previous confinement for parental abduction. I confirmed that the father had full custody of the child, and that a police report was made three days earlier

about the mother failing to return him. I immediately contacted the father and local police in that area. I learned a valuable lesson, which is to always research both the victim and offender.

While researching Jane, nothing appeared out of the ordinary. She loved social media, and possessed very active Facebook, Twitter, Instagram, and Etsy pages. It was easy to see how she could be tracked based on postings from every location which she visits. If unable to find her based on live posts, her online history quickly developed a pattern of behavior that could be used to assume her current location. She appeared very close with her family, and a bit spoiled by her father. As a family with means, she obviously never went without any luxuries, and large gifts for every occasion were normal in her life. My immediate concern was that she would not be able to give up the online activity in order to protect herself. She was accustomed to immediate selfies the moment she receives a new gift or lands at a new vacation destination. She was in for a rude awakening.

That evening, Jane called me from her father's Wire account as instructed. This time, we connected via the video chat option. I wanted to assess her demeanor and look for visual signs of physical abuse. She was very shaken and had slurred speech. Her father warned me before the call that she had been drinking alcohol heavily lately, and today was no exception. He firmly believed that she would sober up once she was safe. As we talked, her father stayed right by her side, which was a problem. She was holding back details that she did not want him to hear. I politely requested to talk with her alone, which he prohibited. He quickly reminded me that he was paying for my time, and that he would be involved in every step.

I instructed her on how to turn on her new iPhone without attaching it to any previous accounts. I had already created her an anonymous Apple account that would allow her to download any basic apps and updates that she might need. We configured the Wire and Signal apps on her new device, which she could use over Wi-Fi only at this point. I had already ordered her a new Mint Mobile SIM starter pack from Amazon that would arrive at her father's house the next day. She was instructed to send me the details of the card, and I would activate it online for her. She would only need to enter the SIM card into her phone and have a clean device ready for communication. We would finish setting up the phone the following day.

Her father insisted that she would be safe at his home for the rest of the week. While the boyfriend likely knew she was there, he had never made contact at that location since the break-up due to the father. He was not shy to pick up a weapon at first glance of Chris entering the property. I knew that the father would likely be at work the next day, so I ended the conversation until then. I hoped that I would be able to talk to Jane alone in order to get the real scoop.

The next day, I received a Wire message from Jane stating that she had the SIM card and was ready to activate. We connected over Wire and finished the process. She was alone in the

house, which gave us an opportunity to talk candidly. Over the next hour, I learned details about her life which her family would never want to know. I learned about the hard drugs, the weekly routine of passing out and waking in an unknown bed, and the monthly breakups with Chris. She told me of the two occasions in which he raped her, which she never reported. She showed me the scars from the cigarette burns purposely placed on areas of her body normally covered in clothing. I asked the difficult questions such as why she continues to go back to him. She answered honestly with “for the drugs”. Chris was not only her lover, but also her drug dealer. She was allowed a non-stop buffet of various drugs in return for their relationship. Chris needed to go away for many reasons.

Jane was adamant that she was ready to go to rehab and leave Chris permanently. He had told her on numerous occasions that he would kill her if she ever left him and that he would never stop hunting until she was dead. He was mentally unstable, fueled with drugs, and possessed a large amount of cash from his illegal transactions. He was a valid threat. With her father funding the privacy campaign, I was ready to execute various strategies. The first priority was to get her the help she needs. It was time for rehab.

Sending Jane to rehab sounds like a simple task. Drive her there, drop her off, and send the bills to her father. It was not that easy. In Jane’s part of the country, there were not many rehab options. Chris would have no trouble contacting each facility and using social engineering tactics to identify the location of her stay. For those that are not familiar with the term, social engineering is psychological manipulation of people for the purpose of performing actions or divulging confidential information. It can be simplified as lying during a con. I have used this tactic many times on behalf of clients.

A call by Chris to each rehab facility during a weekend evening, when newer staff is likely to be present and administrative personnel are not around, consisting of a few targeted inquiries, is likely to quickly identify her location. “Hi, I am Jane’s brother. I was there earlier today to visit, and I left my inhaler there, do you have it? I can’t get a replacement until Monday”. This will be met with either, “We don’t have a patient here with that name”, or, “I don’t see anything at the desk, let me go check her locker”. Chris would be in her room within hours. She would be either dead, kidnapped, or sedated with illegal drugs before sunrise.

I convinced the father to place her in an out-of-town rehab facility that often caters to celebrities. These institutions are more likely to block amateur attempts at obtaining patient information. They know the tricks and are suspicious of every phone call. Their security is better than the average clinic and the place I chose does not allow any cellular devices within the buildings. He agreed, and she began packing. This was equally beneficial to me as it would give me time to set up her new life.

I purchased Jane a one-way airline ticket to the city of her rehab using a prepaid credit card purchased from a local CVS pharmacy. I chose the Vanilla Visa reloadable option. The maximum card value available is \$500, but an additional \$2,000 can be added to the card each day in \$500 increments. Therefore, I can walk out of the store with a \$2,500 balance on the card. Why not just use her real credit card? I must assume that Chris has access to her statements and activity. A simple keystroke logger on her laptop, or malware on her previous phone would give him her passwords. Monitoring her credit card activity would tell him the flight number, which would identify her future location. This would give him a great advantage. Today, airlines are more cautious with prepaid card purchases. If replicating this today, I would use a Privacy.com account.

I hired a car service to transport her from the family home to the airport. Before picking up Jane, the car would pick up Jane's escort, an off-duty police officer from a neighboring community. For several years, I had been teaching open source intelligence (OSINT) techniques to local, state, and federal law enforcement agencies all over the world. This has created a massive private list of contacts covering most areas of the country. I reached out to a woman who I had met at a class and asked if she would be willing to take a day off of work in order to make some side income. She agreed, and escorted Jane to the TSA checkpoint.

The reason for the escort was two-fold. First, I wanted someone with Jane in case Chris appeared during transit. I also wanted that person to be armed with a gun and have the training to use it. While this scenario of Chris intercepting transport is extremely unlikely, I prefer to be prepared. The more likely reason that this officer would be needed is to make sure that Jane makes it to her flight. I still did not trust that Jane would not willingly disappear looking for drugs. I would expect to hear that Jane never made the flight. Therefore, her escort was there for the entire process, and even waited at the only terminal exit until the flight had taken off. I was happy to give this officer twice her daily wage for a few hours of work.

Upon landing, I repeated the process with an off-duty officer working for the airport police department of that area. He picked her up at her flight's gate and escorted her to the vehicle service, then the vehicle, the entire ride, and to the front door of the rehab facility. I received text updates throughout the entire day. Everything went as planned, there were no hiccups, and Jane was safely at rehab. The security team there was now in charge of her. This is one of many reasons that I try to collect as many business cards as possible at my live training events. Contracting local off-duty police officers is my preferred option every time, especially those that I have met during my classes.

Now that she is safe at rehab, my work begins. I must secure permanent housing for her, as she may only be in rehab a few weeks. This is where I try to provide value to my clients. I establish a new life that they can simply walk into without much effort. I create new aliases and establish believable histories that allow people to feel safe in their own homes. It is vital

that any actions I take associated with Jane's new life have no attachment to her previous existence. This is easier said than done.

The first step is to establish housing. Jane's situation is an ideal case for renting. Her father will pay the rent, and she will not stay at this new place long-term. When I create a relocation plan that includes a rental property, I always plan for the client to be present at the location for one year. In most situations, they relocate to something more permanent before the year is up. On rare occasions, they need to extend their situation past the first year. Compared to the purchase of a new anonymous property, establishing a rental unit is much simpler.

Since I will not be providing my client's name or personal details, the thought of obtaining a commercial apartment is out of the question. These large complexes are always controlled by a third party or national chain. They will always require a full background check including the client's SSN and DOB. An occupancy permit will be filed with the city or county, and there is no way to establish privacy in these situations. Therefore, I always focus on properties available for rent by the owner. Preferably, I desire small homes situated on the owner's primary residence property. Since the owners will always be physically next to the unit being rented, they know that they can keep an eye on things, and have a stronger sense of control over the property. This tends to give them a sense of security and in return lowers their concerns to overly vet a new tenant. In a small town, finding these properties requires an afternoon drive and a keen eye for signage. Larger cities require the internet.

Zillow does not offer a specific search for rental housing available strictly by owner. However, a few tweaks can eliminate the larger commercial properties in which I have no interest. After selecting "Rent" from the main page, I select "In-Unit Laundry" from the "More" tab. This eliminates many of the multi-unit properties that share a common laundry area. I then deselect everything but "Houses" on the "Home Type" option. This works best on most areas, but will not work on extremely populated urban areas. I always guide my clients toward areas with a bit of privacy, such as a standalone residence. I then compare the areas of interest to various online crime maps in order to identify the safest area of town. Identifying homes that would be acceptable to the client is not the hard part. Finding landlords that will play nicely with my antics is the difficult piece.

Once I find a home of interest, I contact the owner in person. I arrive well-dressed and in a newer rental vehicle. I politely tell them that I am searching for a friend, and that we are ready to rent right away. I am usually met with an application at this point, which is when things will go one of two ways. My first few attempts at obtaining anonymous housing for victims were disasters. I incorrectly assumed that the landlords would be fighting over me and the money. I strongly stated that I would not disclose the name of the tenant and that we would be providing no identification. You can guess how that went. I slowly learned that a specific delicate approach tends to work most often.

In this scenario, while home-searching for Jane, I found a perfect one-bedroom house tucked back in a wooded area. The home sat on the corner of three acres, opposite of the property owner's home. The home was vacant, and the owners proudly walked me through the recent updates. It was then time to lay out the situation.

I advised the couple, both retired and in their 60's, of the situation. I disclosed my real name, and offered them my retired credentials and badge to verify my identity. I also advised they could Google me and confirm the type of work I conduct. I informed them that I am seeking a small quiet home for a woman that has suffered a lot of mental and physical abuse. She has become fairly skeptical of the world, and has asked me to deal with housing. It is vital that her name is not associated with the home or this address, and it is a matter of her own safety. It could literally be life or death.

As I saw the brows of the owners display the concern on their minds, it was time to sweeten the deal with the following statements. "I realize that you will be very strict when selecting the tenant for this amazing property. I truly hope that you will consider her, as she would be a respectful and quiet tenant. I know the situation is unique, and I would share your same concern if I were in your shoes. This is why we feel the need to compensate you for your consideration. I am authorized to pay the rent in cash each month, plus a deposit, and prepay three months of rent as a gesture of appreciation". This usually converts the look of concern to images of cash in their pockets. While this does not work every time, it usually opens the door for further negotiation. On one occasion, a landlord responded with "Make it six month's cash, in advance!" I happily agreed and my attorney handled all of the paperwork.

This brings up an important point to consider. Obviously, the client's name does not get associated to the property whatsoever, but neither does mine. I have property attorneys on each coast that take care of all rental paperwork and happily attach their own names and signatures to any forms. Neither of them cares about their own privacy, they each use their public office addresses, and neither of them ever know the identity of my client. They each receive a nominal fee for their one or two hours of light paperwork (which they likely have an intern complete).

At this point, you may be thinking that this all only happens because the client has money to throw at the problem. While this is true in this situation, it is not always the case. I have had many clients that did not have a penny to pay, but still received my services without charge. I have also had extremely wealthy clients that pay the lion's share of the bills.

The owners agreed and I now had a rental property lined up for Jane. Two days later, I had the keys and legal possession. During the previous walkthrough of the property, the power, water, and gas was active. I knew that utilities were not included, but I incorrectly assumed that the bills would stay in the name of the property owners. This had been the case with my

previous client relocation, and the landlord just added the usage to the monthly rent. This is always the optimal route to go. In hindsight, I was so excited that they agreed to waive the background check and application process, that I got ahead of myself and just wanted to get a contract signed. This was not a huge issue, but I was very disappointed that I had not clarified this. As I stood in the living room of Jane's new home, I was without power or water. All utilities had been terminated as of the move-in date.

The next morning, I first contacted the power company. This is never an easy call. Traditionally, establishing power to a residence requires a "soft pull" on a person's credit report, which demands a Social Security Number (SSN) of my client. Some may wonder why I would not want to share this information with them. The simple answer is that the details provided will absolutely become public record at some point. Data mining companies often obtain utility records in order to better populate their databases on practically every citizen. The name on the utility bill will likely be present on free people search websites within ninety days. Therefore, disclosing my client's identity to the power company is not an option. Instead, I will test the waters one piece at a time.

Since I record all of my telephone calls as they relate to a client, I am able to provide an exact transcript of the conversation. The following occurred in Spring of 2017.

Operator: Hello, how may I help you today?

Me: Hello, I need to activate power at my residence, can you assist?

Operator: Absolutely. What is the address?

Me: REDACTED

Operator: OK, I do see that this address is part of our coverage area, and that power was terminated on Tuesday. When do you want the power activated?

Me: Right away if possible, we are moving in today, and my daughter is so eager to get the PlayStation going.

Operator: What is your name sir?

Me: John Arthur Wilson

Operator: And what is your date of birth?

Me: Hmm. I really hate to give that out, I was the victim of identity theft this year, and the officer advised to never give out my DOB or SSN. What are my options?

Operator: Sir, I cannot turn on the power without your information including your social.

Me: Oh boy, that is concerning. I am happy to pay a deposit to my credit card in order to bypass this valid requirement. Is there a supervisor that can authorize this?

Operator: Sir, I can tell you most certainly that we cannot turn on the power without your full information. A supervisor will tell you no different.

Me: Understood, let me call you back after my wife gets home.

This conversation was typical. Utility companies want to be sure that you do not rip them off and leave with an unpaid bill. By conducting a credit check, they can come after you when you owe money. In about half of my attempts, I am allowed to pay a \$250-\$500 deposit in order to bypass the credit check and SSN requirement. Usually, I can provide a credit card to pay this, but sometimes they will want a check mailed. I am prepared for either scenario with a secondary credit card that I maintain in an alias business name or a check with no personal name or details in the upper left corner. Both are valid payment, and connect to a business checking account in the name of an LLC that I maintain solely for this purpose. I then invoice the client for these expenses.

After waiting a few minutes, I called the power company again and was given a different operator. The conversation was similar, but I took it a new direction, as follows.

Me: Yes, I am trying to help a foreign exchange student obtain power at a rental home. My English is a bit better than hers, so I thought I would assist.

Operator: What is her name?

Me: REDACTED TRADITIONAL INDIAN NAME

Operator: Does she have an SSN?

Me: No, she says she has a UIDAI National Identification Number, can she give you that?

Operator: Sure, go ahead.

Me: 5485 5000 8000

Operator: OK, so, just so you know, she is going to have to pay a \$200 deposit, which can be refunded after one year or when she terminates service, does she have a credit card for this?

Me: I am happy to pay that for her, are you ready for the number?

Everything was smooth after that point. Before you judge me too heavily as a fraudster, let me explain. The Indian government assigns a twelve-digit national identification number called a Unique Identification Authority of India (UIDAI) number. On their website, and an example of this number is displayed on a fictional card as 5485 5000 8000. This number will never be assigned to any individual. Furthermore, the U.S. utility companies have no way of verifying this number as valid. Operators likely just add it in the notes section to cover themselves.

Think about it. Thousands of foreign exchange students enter colleges and universities every year. They all live in some type of housing that requires utilities. Most of these require the student to pay the utilities directly. Therefore, it is a common occurrence for non-U.S. citizens to activate power at a residence. Starting with this excuse has been more successful than trying to make an employee understand that you prefer not to identify the homeowner. At the end of the day, all of the bills are paid, we have stolen nothing, and the utility companies are happy. No one ever checks up on this situation because there is no need. I make sure the bills are always paid in a timely manner.

The water, sewer, and trash services were much easier. After they were notified that the power had already been activated, they seemed content that everything was legitimate. I set all three services to auto-pay to an anonymous debit card created specifically for this client, and provided a very generic name. I used Privacy.com, as explained previously, which connects directly to the victim's personal checking account. After association, users can create an unlimited amount of debit card numbers, each used for a single merchant. Any billing name and address can be used during payment, and the transactions are withdrawn directly from the checking account on file. The merchant (utility company) does not know the true name of my client. The service (Privacy.com) does know the name of my client, but does not know where she lives. They only know that she pays various utility companies monthly. There is obviously a paper trail here that could be identified with a search warrant or court order, but those are not my concern. I need her out of public view.

The house was ready for Jane in plenty of time for her release from rehab. It was now time to train her on the use of her new aliases. Choosing an alias name can be difficult if too much effort is wasted on finding the perfect option. I don't buy into that, and I don't get overly creative with picking aliases. Why does she need an alias name? She can never associate her true name with her residence. She will need something to use in place of her given name.

I almost always recommend that a client maintain their actual first name as part of their alias. The exceptions are very unique names which would be easy to find with targeted searching. Jane is a common name, so it will work fine. Also, she will naturally respond when called, and will not create an awkward situation when she can't remember her alias name. She cannot ever use her last name, so I often recycle the last name of either the previous resident or the landlord. In this case, assume that the previous resident was also named Jane Doe. This would not work, as it is too similar and mail could be accidentally forwarded to the previous resident. If the previous resident was named Jim Watkins, then Jane Watkins could be a good choice, unless Jim has a family member with the same name. A quick search through various people search tools immediately identifies relatives' names. If the previous resident's last name is not working out, or is very unique, I will focus on the landlord's last name. In this case, the landlord was Matthew Parker. Therefore, Jane Parker will work great.

Why not choose a random last name? There are a few reasons, but the most important is familiarity. If Matthew Parker owns the property, and is publicly listed on many websites, another person there with that last name is not suspicious. The mail person will not think twice about delivering mail to a person with a last name matching the property owner, who also receives mail on occasion. Also, it helps hide the fact that a new resident is present. If this is a small town, it would not be difficult to search for any new residents within the past month. This could unnecessarily expose my client. Maintaining the last name of the property owner or previous resident is just much simpler. There is one other reason.

In a perfect world, my client would only pay with cash, buy all necessities from the local store, and never attach her real name with any purchase ever again. We don't live in that world. We require Amazon accounts with Prime shipping, and practically every big-box store will require a name and other details for large purchases and deliveries. It is almost always certain that the databases that store these details will be breached, sold, or somehow released publicly at some point. Therefore, we must be prepared.

First, I created a new Amazon account in the name of Jane Parker. I supplied the real address to her home, and Amazon conducted a public records search as part of its fraud prevention actions. Having the last name of the property owner can often bypass any red flags present when it can't verify Jane Parker is a real person. Amazon seemed happy with the details, and the account was ready for funding. I did not provide a Privacy.com masked debit card number to this account, as these are detected by Amazon as suspicious when attached to a new account. Instead, I purchased an Amazon gift card from the closest grocery store to the residence. Amazon knows where these accounts are purchased, and buying in one state while using in another is also a red flag.

I attached the Amazon gift card to the account and made a small purchase. This is below the threat model that scrutinizes first purchases, and I selected the option for a free month of

Amazon Prime. The item arrived quickly, and my client now has history with her new alias and new address within their system. I chose the option to purchase Amazon Prime for an entire year and used the remaining balance of the Amazon gift card to pay the fee. This makes Amazon happy, and their systems become much less cautious of the account. At this point, I add a new Privacy.com masked card to the account and make it the primary form of payment. Jane can use this account to buy anything she wants from Amazon, and the transactions will be withdrawn from her personal checking account behind the scenes.

This process can be replicated with any other online shopping options, choosing a new Privacy.com card for each purchase. Within a few months, data mining companies will assume Jane Parker is real. She will even start receiving junk mail at the house. I see this as a sign of success. She has committed no crimes, compromised no one's identity, and paid all of her debts. She has no photo identification including this name (yet) and will never identify herself as an alias to any government official. She knows the rules. More importantly, she will never tell anyone she does not know that she is Jane Doe.

Using an alias on the internet is easy. Online shopping is an interaction between your computer and another computer. Neither cares about much except whether you have a valid form of payment or you are a fraudster trying to rip someone off. As long as we keep the systems happy, we will likely never be stopped. In-person purchases are a bit trickier. In my youth, I paid a cash deposit for my first apartment, and wrote a check at the local furniture store for a couch and kitchen table. I was never asked for identification. Today, paying cash for large items is criticized and any large purchase requires a valid government ID. Let's tackle both of those issues.

Now that Jane was healthier, I snapped a few boring face-forward photos of her standing in front of a white wall. Each had her wearing a different shirt and her hair in a unique style. These will be my starting point for creating her first ID in her alias name. Before you get bothered by this, please let me explain. There will be very rare instances that she will need this, and we will be sure not to break any laws during the creation or utilization of these IDs.

When we think of "Fake IDs", we often have thoughts of underage kids buying a poorly made driver's license with an unbelievable date of birth. That illegal act is never tolerated by me in reference to alias IDs for my clients. Instead, I strictly use the following guidelines which are repeated from an earlier chapter. Please note that some state laws vary, and that I am not an attorney.

LEGAL: Non-government identification in an alias name can be legal. There should be absolutely no mention of any state or the word government. There should be no mention or reference to any real businesses. It should not identify you as an employee of a legitimate company.

NON-LEGAL: Any false identification that displays the words city, county, state, government, police, license, driver, court, agent, et cetera is a crime. This should be obvious. Any reference to employment by any government agency is also illegal. If any part of you thinks that you might be crossing the line, you probably are. Please stop.

I hesitate to discuss the option of printing my own alias identification cards in detail because people may try to break the law and create fake government IDs. Lamination machines and holograms are very affordable on Amazon and local print shops will happily laminate anything you print yourself at home. There are many templates of various styles of photo IDs online, but most are illegal. For Jane, I have a legal solution in place that will assist with convincing others of her new alias name. I made her my employee.

I own a legal LLC business entity that accepts no income whatsoever. Therefore, it does not require an EIN with the IRS and there are no tax reporting requirements. It has a very generic name that could apply to many different industries, similar to Premier Solutions LLC. Jane became a volunteer assistant for this LLC and received no compensation. As an associate of Premier Solutions, I demand that she possess an employee identification card with her photo and name. Since we are a very fun company, every employee chooses a “stage name”, and Jane’s happens to be Jane Parker. I created a new identification card through a template on my laptop, inserted one of the photos I captured, and printed the file to my IDVille card printer purchased from Staples. The ID was printed onto plastic card stock which had the same quality as many government issued IDs.

Possession of this card is not illegal but attempting to falsely identify herself as her alias to a government employee is a crime. Where would she need this? Checking into hotels and receiving packages first come to mind. I advised her to keep it hidden in a wallet, and never remove it unless absolutely necessary.

Aliases possess an unfair reputation as being shady or criminal. While this unfortunate use occurs, an alias itself is not illegal. As long as you do not cross the line of any sort of government identification, you can be anyone you want. It is not a crime to give another civilian a fake name. If I were to visit a Starbucks, I would not give out my real name. There is no benefit. If I entertain a group of clients at a restaurant, I do not provide my real name to the establishment. They do not need that. They only need payment for the services in the form of cash or a secondary credit card. I do not want my clients’ true identities within their databases and guest books that will eventually be breached and leaked online. While this may seem overly cautious, I am aware of the daily breaches and intrusions into sensitive data stored by third parties.

When a client has a legitimate need for identification in an alias name, I encourage them to seek out their own IDs that can help “pad” a wallet. I have found many national chains of

gyms that issue a photo identification card that can be shown for entry into any gym location nationwide. I have had great success using this as a valid proof of identity at hotels. Many of these businesses will give you a 30-day free trial in order to evaluate the property. Of those that I have tried, some of them issued the identification card with photo. I have also found a handful of spas in affluent areas that possess a monthly usage business structure. These also mandate that members show their spa ID upon arrival, most with photo on the card.

Animal shelters are becoming more aggressive about security and often ask volunteers to wear an identification card while on premises. Obtaining an alias photo ID from a shelter as a volunteer has many benefits. First, volunteering and caring for the animals is a nice thing to do. Also, showing this ID when checking into a hotel often sparks a conversation with the receptionist about his or her animal history, and it creates a calm and welcoming environment sure to pacify corporate policies about valid photo identification.

Now that Jane had her invisible home, new alias name, and photo identification, it was time to issue her a new credit card. This is actually one of the easiest steps, which surprises many people. We wrongfully associate our credit cards with a belief that they can never be legally used by other people. Any of us can give a credit card to someone else and authorize them to make a purchase. While a merchant may not accept use without identification, there is no fraud. Similarly, we can use a credit card in someone else's name. However, there are some very serious caveats to this, as explained previously.

Many married couples possess two credit cards that are connected to a single account. They may possess the exact same account numbers and expiration, but they display different names for each spouse. One of these cards is associated with the PRIMARY account holder, while the other is a SECONDARY issue card. This can also be true for children. Many parents add a secondary card to their account, place the child's name on the card, ship them off to college, and hope for the best. If you have ever ordered a secondary card for an account, you have likely noticed that there was never an inquiry for an SSN for the cardholder. This is because it is only a secondary card. There is no need for a credit check because the primary card holder is responsible for all charges. Theoretically, you could add a secondary card in practically any name to an account, and any purchases with that card would simply appear on the primary credit card statement. We can use this as a strategy for privacy.

There are only a few major credit card companies that offer secondary cards without much resistance. Of those, Chase and American Express are two of the easiest. Unfortunately for me, Jane does not have either of these cards. Instead she only has a US Bank credit card. The major banks, such as US Bank and Bank of America, will not issue secondary cards to an account without a full vetting of the new cardholder, including SSN. Jane was willing to apply for a Chase card, but I had just established her credit freeze, which prevents any new inquiries. This important strategy was previously discussed. Therefore, I had to un-freeze her credit,

apply for the new card in her father's address, and then re-freeze her file. This is not a huge deal but added a few days to the process. Once she had a new Chase card delivered to her father's address, it was time to add a secondary account.

An important step to this process is to never use the original card in the real name. Any secondary cards will have the same account number, and we want to keep a bit of distance between the names used. I immediately destroyed her card to prevent temptation. After instruction and a rehearsal, I had her call Chase about her account.

Chase Operator: Hello, how may I help?

Jane: Hi, I just received my new credit card, thank you so much! My previous provider issued me a second card for my step-daughter in college, is that possible with this card? I just want her to have something for emergencies.

Chase Operator: Absolutely, what is her name?

Jane: Jane Parker. She has my first name and her father's last name.

Chase Operator: Before issuing this card, I must make you aware that all purchases with this card will be charged directly to you and you will be responsible for all activity. Do you still agree to having a secondary card issued to your account?

Jane: Yes.

Chase Operator: OK, the card will arrive at the address on file to your account, it will be addressed to you, and will arrive in a plain white envelope.

In three days, the card arrived at Jane's father's residence, and she now had a credit card in her new alias name. There is obviously a connection between these two names now, but only Chase knows this. Chase will eventually include this new alias as a possible associate of my victim, but that cannot be avoided. Having a credit freeze in place will prevent the majority of this leakage.

I do not advise all clients to obtain a secondary credit card. The wealthy clients have many more options such as invisible LLCs with business checking accounts. However, Jane does not have the resources for this. Also, she will definitely need a credit card for daily life, and I do not want her using anything in her real name in the new town where she lives. Therefore, the convenience of having an alias credit card outweighs the risks associated with connecting a secondary card to an alias name.

The final step in Jane's plan was to establish a post office box in her real name at a small post office a couple of towns away from her. She will need access to mail and her bills, and nothing should ever be delivered to the house in her name. I helped her complete the form and supplied only legitimate information. I used her previous address, where she still receives mail, and her real name. The post office does not know her true physical address. Jane was instructed to only use this address for anything that she needed to receive in her real name. It should never be used for her alias. That would connect the two names together further and could jeopardize her home address by associating her real name to any alias utility bills. She could use this PO Box as her address for tax filing and any other government related services. It cannot be placed on her driver's license, but that is not necessary for her at this time. She was still listed under her father's address. Other clients have had to obtain a new driver's license address, often referred to as a ghost address, which was previously explained.

Jane was now in good shape. I was finished. She was clean and sober, lived in a house with no ties to her real name, possessed an alias ID and credit card, and most importantly had a strong understanding of the reasons for all of this fuss. I wished her well, and incorrectly assumed we would never see each other again. She would later reach out to me when Chris showed up.

I take responsibility for this. When I gave her the secondary credit card, I told her to use it sparingly, and only when a credit card was required. I focused on things such as hotels. I did not make it clear that the card should not be used as part of her daily life. As time passed with no sign of Chris, she relied on this secondary card heavily. She used it every week at the local grocery store and for fuel from the local gas station. The credit card possessed a very detailed history pattern. Chris identified Jane's new ProtonMail email address from a common friend. He then sent Jane a phishing attack for which she became vulnerable. She provided her ProtonMail password, which Chris used to access the account. In the archives was her credit card statement. He now knew the general area where she resided. Since he is a psychopath, he traveled to the area and secured a local hotel. He parsed through all of the property tax records for the county and isolated those that matched the properties marked as rental units with the county occupancy division. He now had a list of rental homes with each owner's information. He contacted each owner via telephone and provided the following script.

"Hi, I am Jane's brother. I would like to make her rent payment for next month on her behalf. Do I have the right landlord? This is a gift and I would like to surprise her, so I hope you will keep this a secret for now."

He assumed she would keep using her first name, and he was correct. Most of these calls ended with confusion as the owner did not know "Jane". Eventually he reached an owner which confirmed he rented to Jane and even described her to make sure they were each talking about the same person. He now had a likely address. He conducted surveillance but did not ever catch her in transit. Her recycling bin was in the street, so he removed the contents and

returned to his hotel. In the bags of papers and plastics, he located empty envelopes addressed to Jane at her PO Box. He knew he had the right home. That night he committed a home invasion and was waiting for her when she returned home. A physical attack ensued, he fled, and was later arrested by the local police. These details were gathered by a detective during an interview with Chris. The detective stated he seemed proud of his work.

I learned a lot from this incident, as I had made many sloppy mistakes. First, I underestimated the suspect. I now assume that every adversary is technically skilled and diligent. Next, I should have stressed more to never use any credit card, even a secondary alias card, near your home. This payment history displays a very unique lifestyle pattern that provides a great starting point to physical location. I should have had her purchase high-dollar gift cards from stores far from her home, and then use those if she needed digital payment. Better, I should have enforced the use of cash at all times.

Next, I now consider the alias first name. I usually like to maintain the first name of my client as an alias for appropriate response in social settings. This may not be wise for clients with extreme circumstances. This is especially important for those with unique names. I must now always include the landlord when considering the weakest links in my plan. I should have also stressed the importance of shredding or burning anything with her name the moment it needs to be discarded. Personally, I burn anything with sensitive information, but only after it has run through my cross-cut shredder. This makes for great kindling if you have a fireplace or wood burning stove.

Jane and I learned a lot. She was one of my first abuse clients. I was working in uncharted territory. This is no excuse; these were amateur mistakes with advanced adversaries. Jane has since moved to another home anonymously using similar methods as previously stated. She had one close call when her home address was published to an online marketing website which gathered “leads” through malicious methods. Her name and home address were leaked to this database because she requested a quote from a questionable online renter’s insurance provider which shares data with numerous third parties. The data was later sold as leads for future business. This site had no opt-out policy and requests to the business owner went unanswered. My response was to file a COPPA complaint. I informed the website owner, copying the abuse address for his web host, that he was in violation of the Children’s Online Privacy Protection Act (COPPA) by publishing the name and address of a child under the age of 13. I provided my adult client’s details. The next day, the entry was removed. This was a bit shady, but warranted in my opinion. I have little sympathy for these types of sites, and I hurt no one. Surprisingly, this tactic works often when websites otherwise refuse to remove personal data.

Chris served less than a year in county jail for the home invasion, and he likely continues to hunt her. While I have much higher confidence in my new strategy for her, he still keeps me up at night.

CHAPTER EIGHTEEN

MY SUCCESSES AND FAILURES: JIM DOE

When I became a police officer in 1997, I had absolutely no concern about personal privacy and safety. My home loan and property taxes were in my name, and all utilities were sent to me at the house. I was very publicly associated with my home and was even listed in the phone book. A few years later, I was involved in a high-profile case that made me question my transparency. While it took me a few years to get completely off radar, I was lucky that I never actually needed the protection. This is not the case for many police officers today.

I often get panicked emails or phone calls from cops that either attended my training or know someone else that had. Something has happened in their lives that has created a spotlight on them, and they realize too late that their entire lives are available online. This was the case of Jim Doe. Jim was a police officer in the U.S. who was involved in the shooting of an armed suspect during an investigation. The shooting was later found to be justified after video from a witness displayed the offender pointing a gun at Jim, but that did not matter much at the time of the incident. Before a thorough investigation could be conducted, the public and the media assumed that the officer was wrong and demanded immediate answers. Protests began and media coverage fueled the hate expanding through the city. The focus quickly turned to Jim.

Jim's department refused to identify the officer that was involved in the shooting until the investigation was complete, but that did not help him. Anonymous "hackers" began investigating the incident themselves. They identified all of the police officers from that city through public payroll records. They then eliminated those that were not on duty after personal social network posts displayed them in family settings. The officers on duty the night of the shooting were quickly identified. Calls to the station asking to speak with each of them resulted in the same officer never being available. Officer Jim Doe must be the shooter.

People began spreading Jim's name throughout social media, which the press picked up right away. Online searches through various people finder websites easily identified Jim's home address, phone number, and family members. News crews were stationed outside of Jim's home, hoping to capture a video clip of him walking to his car. Jim was stuck, and his family was afraid to leave the house. At night, protesters began throwing objects at the home and yelled threats toward the entire family. Jim's children could not attend school as they also received threats over the internet. Jim reached out to me for help.

This is a difficult situation. I can't make him and his family invisible overnight, and I can't make the world forget his home address. All I could offer was to help him obtain temporary anonymous lodging and some peace. At that point, we could create a strategy to get his life back in order. The first order of business was to get him and his family safely out of the house without anyone following. This could be difficult as the group of people standing guard at his house was growing every day. Simply driving him away from the home was not an option.

I contacted the local fire chief and explained the situation. He was very sympathetic, as the police and fire departments work together closely. He confirmed that the fire department possessed an ambulance crew as part of the service to the community. He agreed to assist with the safe relocation of Officer Doe. We identified a time during shift change when an extra crew would be available. This was to avoid any disruption of normal emergency service response. At that time, an ambulance with two medics responded to Jim's house. The lights and siren, which were only enabled upon arrival at the home, cleared a path through the aggressive crowd. The ambulance backed into the driveway until it reached the attached garage. At that point, an off-duty officer opened the garage door, which was almost touching the ambulance, leaving only a small opening that allowed visibility inside. Jim and his family loaded into the ambulance and it departed.

While the ambulance drove away, a police car followed slowly, creating a large gap between the ambulance and press attempting to follow. No one would pass the police car on the two-lane road, and the ambulance eventually disappeared. It responded to a pre-arranged meeting spot where a family member was waiting with a minivan. The family loaded into the van and then continued to a hotel the next city over. An unmarked detective car monitored the situation and confirmed that no one had followed the minivan. Step one was complete.

Jim's department photo was leaked onto the internet, and his face was plastered on practically every television in town. I did not want him recognized by anyone at the hotel. All it would take was one careless employee to tell the world where Jim was staying. Traditionally, this could present a problem, as Jim will need to check into the hotel and pay by credit card. Fortunately, there are alternative options for this.

Before Jim's arrival, I created a new Hilton Honors account online in a new alias name. I then made a reservation at the desired hotel using this account and alias. I used my own secondary credit card in order to hold the confirmation, but did not want to place the expenses on this card. Within moments, I received an email from Hilton with the option to check-in online and select a room. I completed this process through the Hilton website, which eliminates the need to present identification upon check-in. It is designed as a time-saving option, but rarely is. A physical credit card is still required upon check-in, which I did not have attached to Jim's new alias. Fortunately, this Hilton property offers electronic locks that can be opened through the

Hilton app on an Android device. Jim downloaded the app to his new burner Android phone, and logged in with the credentials I supplied to him. I needed to work on anonymous payment.

I could not simply use his real credit card as attached to his real name for the hotel payment. That was too risky. In order for him to rest safely, it was vital that no one could connect him to the hotel. Many of his co-workers offered their own cards, which was no better in my opinion. Instead, Jim sent me his credit card details, and I created an account with the online masking service Blur. Blur generates one-time use credit card numbers for any purpose. At the moment of creation, the chosen dollar amount is immediately charged to the real credit card. The benefit of this new masked credit card number is that any name and zip code can be used during any purchase. The disadvantage is the fees associated with each purchase. This would work fine in a pinch, but not long term.

I created a new virtual credit card in the amount of \$500 and supplied this card to Jim's two-night stay. This action allowed me to prepay for Jim's room, which authorized his phone to unlock his room's door without ever stopping by the front desk. Jim and his family walked in the hotel, went straight to their room, and his Hilton app used his Android's NFC connection to unlock the door. The family was now staying in a hotel safely and anonymously. Very few trusted people knew their whereabouts. There was no media hounding them, protesters screaming at them, or rocks smashing their vehicle's windows. It was quiet and created an environment that could be used to regroup. I arrived the next day to begin planning his new privacy strategy.

Jim was obviously shaken, but not nearly as much as his wife. She was a wreck. Jim had the nerve for these types of situations, but it was killing him to see his wife scared. Earlier that day, she had received messages on her Facebook accounts that included manipulated images of her children inside coffins. Combine that with a family of four stuck in a typical Hampton Inn hotel room sharing one bathroom, and you have a stressful weekend on your hands. I don't know any parent that would not be upset.

There is no easy solution to this scenario. They can't stay at the hotel forever and will need to assume regular lives at some point. My immediate concern is always physical safety and short-term anonymous lodging, which I had achieved. The next step is mid-term housing which usually goes one of two directions. Either I establish an option that allows for a longer stay, or I identify friends or family that can support them while I figure out the next steps. Jim had no family homes where he would be comfortable staying, and his wife's parents had passed many years ago, leaving her as an only child. All of his friends were cops, which would never work. Placing them at a co-worker's home could either jeopardize the safety of that officer or further expose attacks to my client when angry protesters decide that any local cop is fair game. It was time to consider extended stay options.

In 2014, I was the keynote speaker at an insurance risk conference, where I met the CEO of a national chain of extended stay hotels. Out of pure luck, I was sitting at his table in a hotel ballroom while I awaited my speaking slot after a few introductions and awards. When I saw his name tag and the company name, I made him promise me that we could talk after my session. He happily agreed and waited for me in the lobby after the event. The free open bar with top-shelf spirits could have also had an impact on his commitment.

I gave him a very brief overview of the disappearing services that I provide, and he was very intrigued. While displaying genuine interest, I could detect a hint of concern from his face over why I was sharing this information. I told him that I often run into check-in issues at his hotels due to strict identity verification protocols. These places can be stricter than a traditional hotel since guests will often stay weeks or months while working locally in various industries. They always want to know exactly who is staying there and who should not be present on the grounds. They also want to make sure they get reimbursed from the companies that are providing lodging for their employees.

Once he interrupted with, "How can I help?". I knew we would be long-term friends. I told him that there are two things that can help me and numerous clients that find themselves in danger. The first is a fast-track check-in option that requires no identity verification, and the second is the same discount that he applies to his big customers. When a typical traveler shows up to rent a room, he or she may have to pay \$160 a night while the fracking employee in town for a few weeks is quoted \$55. He was adamant that he would make sure that I get the absolute bulk rates but was not sure how to tackle the identification issue. I did not necessarily need his plan, as I already had my own. I just didn't know if he would agree.

My proposal to him was to add my company as a customer within his online billing system. I had a legitimate LLC that was not tied to my name, but possessed purchasing power and had a reliable funding source. His company would issue me a customer number and allow me to book rooms online through their partner portal for the discount. I could book rooms that would not require payment from the person checking-in, and my company could be billed after checkout. This was all fairly straightforward and would allow me to receive the lowest pricing. The real power in this proposal was that he would add the following within the notes section, visible during the check-in process.

"This reservation was conducted through the office of our headquarters. Mr. (CEO NAME) has personally assured the guest that check-in will be expedited without the need for any verification of identification or payment. The customer is to be billed Net-30."

He agreed and had his office set me up the week following the conference. It was nothing more than a typical commercial account, but that small note made all the difference. Most employees saw it while checking-in my clients and immediately offered a higher level of service

without ID requirements. On one occasion, my client received great aggravation due to the resistance on providing ID. She asked the reception desk to look for a note on the account, and it was smooth sailing from there.

I logged in to my online portal for this extended stay hotel chain and located a hotel an hour outside of our location. I made a reservation for 30 days and received a rate 75% lower than retail price. I was able to secure a room with a full kitchen, two isolated bedrooms, and two bathrooms. It would not be the Ritz, but it would be better than the current accommodations. Jim and his family began packing.

You may wonder why I didn't just start at the extended stay hotel and avoid the temporary stay at the Hampton Inn. The reason is out of respect to my friend that owns the extended stay hotels. I promised him that I would never send a client that would cause any type of issue toward his company or employees. I wanted to make sure we were clean from any followers that would notify the world that "enemy number one" was at a property owned by my friend. Therefore, I never start at one of those locations. That step needs to offer a clean spot that can be used long-term if necessary.

Jim's co-workers safely escorted him and his family in their off-duty vehicles to the new extended stay option. As expected, they were never prompted for any type of payment or identification, and only had to show the printed reservation confirmation and purchase order created by my company to pay the bill afterward. Neither Jim nor his wife checked the family into the hotel. One of his friends took care of everything and spent less than five minutes in the lobby. They now had a place to call home for a while.

I gave Jim a week to tackle his own issues with his employer and the situation he was in. When he reached out to talk about long-term plans, he asked if I would come see him personally. I would have it no other way. When I arrived, he went straight to the point. "I put my house up for sale, my friends moved all of my belongings into storage, and my wife never wants to set foot in that neighborhood again", he explained in a very monotone, factual voice. "What do we do now?" he asked, understanding that walking into a new home was not feasible financially. I asked him if he ever considered being a nomad, which he did not answer. "Hear me out", I requested, and I started to explain the concept of the official nomad in terms of home domicile in the United States. I gave him the following pitch.

"Imagine you are retired, your kids are grown and out of the house, and you are ready to downsize. Maybe you live in a cold area, and the idea of chasing the sun is appealing. You decide that you and your spouse are going to sell all of your belongings, buy an RV, and follow the weather. You hang out in Florida in the winters and explore the national parks in the summer. You live in your RV and do not have a state to really call your own. This scenario occurs to thousands of people every year, and those couples chase their dreams while enjoying

the freedom of the life as a nomad. In fact, there are three states that recognize a defined ‘nomad’ and provide a home state without any physical residence within the boundaries.”

The skepticism started to break a bit, but he still did not understand how this applied to him. I continued my proposal.

“Think about those retirees. They must possess a driver’s license and an official mailing address which can be used on any government document. These people still exist and must have an address lined up to receive mail, file taxes, obtain a passport, and maintain credit. Florida, South Dakota, and Texas fill the void for these retirees needing an official home base. The beauty of this option is that being retired or possessing an RV is not required. Anyone can become a nomad, as long as you obey all of the laws surrounding this option.”

My ideas were starting to click with him, and the questions began to fly out of Jim such as, “Is it affordable? Can I have a driver’s license without my home address on it? Would this buy us some time to figure out the next steps?”, and many others. I responded “Yes to all”.

Jim was the perfect candidate for nomad conversion. He was in a tough predicament and needed time. It would be months before any investigation was complete. He had nowhere stable to stay. He was not sure what the future held. He did not know if he would need to move out of state or if the day would come where he could return to the town where he worked his entire career. Ultimately, he was in no place to make any type of commitment and needed to float for a bit. I laid out the entire process of becoming a legal nomad and the entire family agreed to cooperate with the plan. The remaining content of this chapter details every step, including my mistakes made along the way.

I had personally become a legal nomad a couple of years prior to this incident. I always make myself the guinea pig for all of my weird ideas, and this one needed to be bulletproof before I offered it within my menu of services. In 2014, I took an early retirement from my law enforcement job as a cyber-crimes detective. I sold my home and accepted a new position that would have me traveling extensively. I would no longer be an Illinois resident, but I would also not be connected to any other state. I would be a bit abandoned. I could have easily kept my Illinois driver’s license and used a local PO Box, likely not drawing any skepticism, but it felt odd. I had always used the address of the local police department on any government identification, and that seemed inappropriate after retirement. The last thing I wanted was to ruffle any feathers with my previous employer as I started a new venture. After much research, I settled on becoming a nomad within a nomad-friendly state.

My four goals for Jim were as follows, with the reasons for each included.

Obtain a new physical address. Jim will be selling his home, and he would be legally required to provide his new address to the Department of Motor Vehicles (DMV) upon sale. The moment he supplies the actual place he is staying, it is public information. Most states offer some type of option to purchase various databases. Third-party data mining companies love this, and the state makes a nice profit from our personal details. Within thirty days, the address provided will be available on premium people search websites at less than \$15 per query. I can't allow that. Therefore, I need a physical address that can be used on a driver's license, passport application, tax return, or any other legal document. It must also be an address where Jim will never visit. Finally, it must all be legal.

Possess a reliable mail forwarding service. I will be forwarding Jim's postal mail away from his home to a commercial mail receiving agency (CMRA). This will also be public information. Therefore, I need a service that will securely accept all of his mail and send in bundles to any address I specify. This middle-man protects the final destination from public view.

Mislead anyone hunting him or his family. I must purposely pick a physical address that would never be used as an actual residence. I have met privacy seekers that pick random houses and claim they live there. This is irresponsible. I don't want an activist to fire-bomb some innocent person's home thinking they are getting revenge on Jim. His new "home" must be an obvious commercial property that will confuse anyone that spends the resources required to identify the location. He will never set foot anywhere near the location.

Buy as much time as he needed. Finally, I need a solution that will give Jim some breathing room. Becoming a legal nomad can be temporary or permanent. Jim and his family will not need to rush into any long-term commitments and can let this whole situation unfold naturally.

For the sake of this chapter, assume that Jim chose South Dakota. The first step toward establishing residency in a nomad-friendly state is to purchase a Personal Mail Box (PMB), as previously explained. I was able to create an account online in his real name and use a Privacy.com masked debit card to pay for the purchase. Every PMB service I have found possesses awful online security, and I suspect that each have had a data breach of some magnitude. Therefore, I never provide a personal credit card number.

For \$300, I obtained a new physical mailing address, mail collection services, forwarding options, and enough postage to easily cover outgoing shipments of mail for the next year. This is a vital first step toward obtaining true privacy with a "ghost address". From this point forward, any time that my client is asked for a physical address by any government or private entity, he will provide this new PMB address. While most PO Box addresses are not allowed on personal documents, such as a loan or driver's license, a PMB is allowed.

Once the PMB is established, it is very important to conduct a test. I sent a letter without a return address to my client at the new PMB address. The package I chose for Jim included a mail scanning feature which emails him an image of the cover of every piece of mail as it arrives. This is a great feature that I enforce with all clients. It is important to know when mail arrives and needs to be addressed. Within a few days, he received notification of the letter, and we were in business. On one occasion, I simply assumed that a PMB was properly created for a client. Due to a bug in the outdated online system, she was given a different box number which did not exist. She missed some important notices from a government agency which caused quite a headache. This was my fault for not testing. Fortunately, a letter to that agency directly from me accepting fault was sufficient to get her back on the right track. I now test all new PMBs.

As stated previously, these PMB services are mostly used by retired couples traveling the world in an RV or pop-up trailer. The privacy policies associated with customer accounts possesses the same security that you would expect from your grandparents. On numerous occasions, I have called the PMB company of my clients, stated I was them, and asked them to read the return addresses of all mail pending in the box. I have never been denied this invasive request. As a test, I once called the service and provided a random PMB number and stated that I was missing an outgoing shipment. The representative quickly provided me the last shipment date and address where it was sent. The security at these places is outright awful. However, I don't have a better solution. Therefore, we will get creative with the shipment address of the bundled mail packages.

Eventually, Jim will buy a new home anonymously and he can open a traditional PO Box a town or two away from his home. He can then have the PMB packages sent to the post office. Until then, he needed to receive his package, and I couldn't take the chance of an adversary calling the PMB company to identify where his shipments were being sent. Therefore, I created a temporary solution.

I contacted an upscale hotel a few miles away from his current extended stay location. I made a one-night reservation in his real name for two weeks from the current date. I secured it with his real credit card and confirmed the cancellation policy. I then requested the PMB to ship all pending mail to my client at the hotel address. Tracking information identified its arrival, and his wife went and picked up the package. She stated that she had an upcoming reservation, but she wanted to pick up a package that recently arrived. The hotel staff verified her identification and retrieved the item from storage. After she had the package in hand, I canceled the pending reservation without any charge on his card. Why did I have to be so sneaky?

If someone convinced the PMB company to disclose the shipment location, this plan did not impact my client's immediate safety. Realistically, no one will ever know any of this happened.

If an adversary identifies the locations of shipped mail a few months later, he or she will waste a lot of time determining if my client is still at the upscale hotel. By then, he will not even be living at the extended stay option twenty minutes away. It is an ideal temporary fix. If I had sent the package to the hotel without making the reservation, it may have been rejected as "Return to Sender". Finally, the PMB is mandated by USPS rules to only ship packages in a confirmed name. Every shipment that Jim requests will have his and his wife's name as the recipient. This needs to be kept in mind at all times, and Jim will need to be selective about delivery.

I must confess that this idea of shipping to random hotels did not come to fruition proactively. It was a reaction to an unpleasant situation of my own. In 2015, I forwarded my PMB mail to an address of a friend whom I would be visiting. The package was delivered to his home in my name before my arrival. I obtained the package during my visit. He had no concerns about privacy and had no objection to me receiving mail at his place. I didn't think anything of this for weeks after my departure. That lack of concern faded away quickly.

My PMB address is publicly available through data brokers such as CLEAR. This is by design. It is an address that can be publicly connected to me without fear of compromising my true location. Someone identified this address and contacted the PMB provider, pretending to be me. The service provided this intruder the last address where a package was sent and a list of pending mail waiting in my box. The subject then attempted to social engineer my friend. He stated that he was with the PMB provider and that a package had been returned undeliverable from my friend's address. The subject then asked my friend where he could send the package so that I could receive it overnight. My friend honestly responded that he did not know my home address, and the attempt failed.

I learned two valuable lessons. First, never forward mail from a PMB that could compromise you. Send it to a UPS store or a hotel. This eliminates a personal attack surface. Next, I learned that your friends and family can be the weakest link. If my friend had fallen for the attack, the intruder may now know where I live. To this day, I have no idea who the person was. I only received an anonymous email soon after my friend told me about the call. The subject confessed to his actions but never disclosed his motivation. OK, back to Jim.

The only negative response to this scenario is the mischievous feeling of accomplishment by Jim's wife. After she received the forwarded package at a hotel where she never stayed, containing out of state vehicle license plates from her "ghost address", she was hooked. I had created a monster. In her mind, she was Jason Bourne, and a bit too excited for the next level. I watched her closely after that. Jim also had the nomad bug when he switched his license plates from the old state to the new. He seemed excited that there was a tangible step in the right direction, and he seemed to have a sense of a future solution to all of his problems. Next, it was time to make them official residents of the state of South Dakota.

The eight-hour road trip was full of excitement. Jim and his wife interrogated me on the next steps and other levels of privacy they could achieve. I shared a bit about my personal strategy and gave them some insight into the next tier. More importantly, the drive gave me time to prepare them for the various roadblocks they would face after this next task. We talked about address change notifications, credit freeze problems, insurance issues, and a slew of other complications they had not yet considered. I assured them that I had solutions for them, but it would not always be easy. Their lives had changed, and they had no option to return to the previous version. There would be many additional hurdles to face.

We arrived at the hotel, where I had arranged two rooms under an alias name. I have not stayed in a hotel under my real name in a decade, so I did not think much of this. Jim and his wife were not prepared. The three of us walked to the counter and I supplied my alias name as a new check-in and waited for the attendant to retrieve the reservation. Jim and his wife simply stared at me with open jaws. I should have told them my plan, as they looked at me like betrayed children. I provided a credit card in the alias name and a rewards card from that hotel chain matching the identity for the reservation. I was not asked for identification, as I had obtained the highest tier of their frequent traveler program. At that level, the rules rarely apply, and the hotel clerk's job is to make the stay as perfect as possible. I had identification available if necessary, but it is rarely required.

My mistake here was not notifying my client of every action. The desk clerk picked up on their looks of surprise at my name, and likely thought I was involved in some illegal activity. I now explain everything at all times, and never present any surprises.

I gave them their room keys and we agreed to meet in the morning for breakfast (free of course, thanks to the rewards status). My friends and family from my home town always seem impressed at the perks I receive when we travel together. The truth is that it is a sad moment when you achieve elite status. It clearly reminds you that you have no social life and that you may be overly dedicated to your work. I would trade in all of my perks in exchange for the lost time due to extensive travels. That is likely the most personal piece you will get from me here.

In the morning, I outlined the plan. I was heavily armed with all of my previous mistakes made in South Dakota, and I anticipated a smooth process. Jim and his wife seemed overly nervous, but I knew the feeling. The day I received my driver's license as a nomad, listing a ghost address as my home, I was beyond thrilled. It was my first experience with the process, and I expected to get arrested. It seemed so shady, but I now know better. I was about to walk two clients through the routine with my head high, confident in my methods and the laws that allowed the process.

There was one hiccup during my own residency process that I will never forget, and which I have never replicated. When I arrived at the DMV to obtain a nomad license, I had no proof that I had stayed the night before in the county of the DMV building. This is a stern requirement that is heavily enforced, likely to make sure the county received the tax revenue from a lodging stay. I had my hotel receipt, but it was in an alias name. I had to leave the DMV, return to the hotel, convince the front desk to print an additional receipt in my real name, and return to the DMV for more scrutiny. I eliminated that alias afterward, as it was now directly associated with my true name within the Hilton system. Another lesson learned.

Before we all left the hotel, I asked the front desk clerk to print two separate receipts for the two rooms. I also asked that she include each of my clients on the independent receipts. I apologized for the trouble in advance and told her, “You know how bosses can be, everything must be perfect”. She gave a nod as if she could relate and issued me two receipts. Jim’s name was on one and his wife’s on the other. We were ready for the show.

The DMV was only a few minutes away from the hotel, and we arrived before the car could properly heat. We sat in the car for a moment and made sure everyone was ready. I told them to follow my lead and assured them that we were about to conduct a very legitimate process. Jim was ready to knock it out, but his wife appeared nervous. We stepped in to an empty DMV building with three employees ready to help. In South Dakota, you are immediately intercepted by a “greeter” who is present to help with the process. There are so many retirees that technically reside in this county, that the bulk of their business is out-of-towners that have no clue what to do. This is very helpful, as it removes the scrutiny on our plans. I opened the dialogue immediately with “Hi Tom, good to see you again!”, before the greeter had a chance to speak. He vaguely remembered me but was not sure why. I continued with “I brought Jim and his wife with me to get them set up as nomads since they just bought their first RV, and our first stop is Mount Rushmore!”, which lit up Tom’s face.

I have found this demeanor to create a great vibe within the office, and Tom likes to tell stories about his own RV adventures. He also happens to be very fond of Mt. Rushmore. This introduction was no accident. Tom works part-time on Mondays and Wednesdays. His work schedule and dedication to the carved presidents is publicly available on his Facebook profile. I have no shame; I will use every resource to my advantage. When Tom is happy, he makes sure that my clients have no issues with their new nomad status.

Tom verified that both Jim and his wife possessed the following documents.

- Current out-of-state driver’s license
- Secondary ID (passport or certified birth certificate)
- Verification of SSN (original card or 1099 form)
- Receipts showing lodging in the county within the past year

- Additional documentation of South Dakota address
- South Dakota Residency Affidavit

Most of these items should make sense for any DMV license transfer. The additional documentation of the South Dakota address is not absolutely required but has been very helpful in the past. Showing your PMB company paperwork with your name and new address is usually sufficient. However, I have had two situations where the DMV employee demanded to see something official associating the person in front of her with the address being requested for the license. This is where the vehicle registration comes in. Since I already registered Jim's vehicle in his and his wife's name at his new PMB address, I had official documentation from the state. Showing the title or registration verification has always been sufficient. If a car had not been registered, I could have presented an Amazon invoice or bill as proof. The most important lesson is to have more than you need upon arrival.

Tom confirmed that their proof of a local PMB satisfied the state requirement for residency, and they could legally call South Dakota their home if they wished. He informed them not to worry about the notification of potential jury duty. If they would be selected, a simple call identifying themselves as full-time travelers who do not actually live in the state would remove them from any obligations. Jim and his wife eagerly signed, and they were ushered toward a DMV clerk. After a quick eye test and photograph, they both possessed South Dakota driver's licenses, and they were now officially residents of the state. While I wish I could discuss the fanfare surrounding this event, there was none. We quietly walked out and returned to the car.

"Is that it?" Jim asked. I confirmed that we were done. He and his wife giggled a bit and I saw a bit of hope in his face. He had been beaten hard by the events over the past month, but this was a sign of a silver lining. We drove 8 hours back to his extended stay lodging and had a closing conversation.

I advised him that the big steps had been taken to buy some time while still maintaining his life's responsibilities. He now needed to take the time to change the mailing addresses on file for every bank, utility, insurance, or financial company that he can think of where he may have an account. Basically, he needs to treat this as a move from one house to another. Additionally, he needed to visit a post office and submit an official change of address form, choosing the "permanent" option on the card. This would forward his mail for several months while he identified other accounts to update. As far as any entity is concerned, his new PMB address is his home.

I should pause a moment and reflect on what this really accomplished. On the surface, he simply possesses a new driver's license and vehicle registration. This alone does not physically protect his family from danger. The power of this strategy is the ability to use it as a tool for future protection. Please let me explain.

While Jim is in limbo and awaiting a verdict in reference to the shooting, he will be on the move. He still needs access to his mail. He still needs to use credit cards and pay his bills. He does not want to return to his home. This solution provided a secure repository for the collection and distribution of mail on his own terms. More importantly, he has a physical address to give to companies that apply scrutiny toward changes of address. If he simply acquired a PO Box and provided the new address to his credit card provider, that company would maintain his last known physical address on file. This PMB address replaces all addresses on file and passes USPS verification checks. Jim can use this address for the rest of his life if he chooses.

It is well documented that states sell driver's license data to third-party companies. The address on your license is publicly available within dozens of free and premium search services. When the next person wishing harm on Jim looks to see where he moved, the only data available will be a commercial receiving service where he has never been present. When he sells his home, the title and transaction forms will be public data. He must disclose a current address during the sale. He now has a safe address to provide where a check can be received. When this PMB is announced in the local paper within property transactions, he has no concern. Jim can still exist, but not be found.

Jim was very selective of the details he was willing to share publicly, and his wife was even less revealing. You may be wondering why I referred to her as "his wife" so much, and never provided a real or alias name. This was her choice. She asked to never be named at all, noting a passage in my previous book *Hiding from the Internet*:

"Be careful when you select an alias name to use. Most people choose something they believe to be random but can actually be very revealing. It might be the name of a celebrity that you like or a distant relative that has passed. Either could be used to associate you to your alias or potential online security questions."

She simply asked to only be referred to as Jim's wife at all times. I respect her decision. Jim would later be cleared in this incident and the shooting was ruled as justified. He left law enforcement completely, and he continues to travel extensively with his family as nomads of South Dakota. The threats died off, but they are still always looking over their shoulders. I consider Jim a success. Things could always have been done better, and I learn from every experience. The protections put into place for Jim had unintended benefits later. The following happened several months after Jim became a nomad.

- An unknown individual attempted to place a "mail hold" on Jim's mail. This is common during scam attempts when the suspect does not want the victim to receive any notifications of financial transfers. Since Jim's mail is at a PMB registered with the USPS, a mail stop was not possible.

- This same individual then attempted a permanent change of address in order to forward future mail to another PO Box. Again, this was declined due to the mail being collected at a PMB. The PMB services do not allow permanent forwarding as you would conduct during a move.
- The suspect attempted to open a new retirement account in Jim's name with his DOB and SSN. Jim received a letter from this bank asking him to remove his credit freeze before any new accounts were requested.
- Someone attempted a SIM swapping attack toward Jim's cellular number which was released during a doxing attack after the shooting. Per the instruction previously, Jim ported his known number to Google Voice and adopted a new prepaid account. The SIM attack was unsuccessful.
- Unauthorized people attempted to make changes to Jim's personal checking account during social engineering attempts toward the bank. The attackers could not identify the telephone number for the account when asked. When the bank called a verified number on file, it forwarded to Jim's MySudo app and he took the call, canceling the changes.

If you were targeted in this manner, would you be protected? I hope this provides enough justification for you to start making changes right away.

CHAPTER NINETEEN

MY SUCCESSES AND FAILURES: MARY DOE

During 2019 and 2020, I witnessed more extortion attempts toward my clients each year than the past decade's cases combined. The ability to mask a true identity on the internet, and the online presence of practically everyone's breached passwords, has created an opportunity for mean people to easily act on their criminal impulses. My online extortion investigations usually fall into one of the following categories.

Stolen Photos: This is the most common scenario. As I write this, I have three pending emails asking for help. Typically, a criminal gains access to online backups of personal photos, usually automated via a mobile device, and identifies any images containing nudity or sexual acts. The suspect then threatens to release the images unless the victim provides either payment or additional nude photos. The summary on the following pages provides more details.

Hidden Cameras: I have represented clients who have been the victim of hidden cameras placed in hotel bathrooms, locker rooms, and other places of potential nudity. The recorded videos are then used for extortion. In one scenario, the victim refused to pay, and the video of her showering was sent to all of her co-workers. In another scenario, a woman seduced my client, brought him back to her hotel, and recorded a sexual encounter. She then threatened release of the video if he did not pay her \$100,000. It was a targeted and well executed setup.

Past Mistakes: In 2020, I assisted two clients with issues from their past. In one, a wealthy business man was contacted by a stranger who claimed to possess a VHS video from 1987 depicting him in an "unflattering way" which could have an impact on his reputation with his company. In the other scenario, my client was sent images scanned from old photographs showing him in "blackface" while in college. After refusing to pay \$10,000, the images were published online and forwarded to the board members of his company.

Stolen Accounts: Occasionally, I meet a client who has lost access to a popular online account to a hacker. This includes celebrities who possess social network profiles with millions of followers. There is a huge black market for these accounts, as they can be used to send spam or harm the reputation of the account holder.

These types of extortion attempts seem to be getting worse. The following pages present my work with "Mary". She and I hope that the details shared here will help others in similar situations.

I met Mary through a Hollywood acquaintance. She is not a household name, but is a very talented actress with an impressive filmography. She reached out to me and we scheduled a call over Wickr. Over the hour-long conversation, she explained the hell she was going through and I began creating a strategy to gain control of the situation. The following outlines every detail of her encounter.

During a Saturday evening out with friends, she received a SMS text message on her iPhone from a strange number. It simply stated “I have your nudes, want proof?”. Before she could respond, the suspect began sending images of her to her phone. These included intimate photos she had taken and previously sent to her boyfriend. She responded with “Who is this?” and the suspect began making demands. He threatened to publish the photos to the internet and send copies to all of her friends and family if she did not pay him \$50,000 in Bitcoin. He advised she had 24 hours. An hour after these messages, she had contacted me for advice.

My first suggestion was to cease all communication and ignore any further messages. In general, I always recommend this. The moment you respond to extortion, the offender knows you have seen the messages and almost always becomes more aggressive. Preferably, no one should ever respond to these. There is usually nothing you can do or say to prevent publication of the images. We were past that, so it was time to begin the investigation.

The telephone number of the suspect displayed a Los Angeles area code, but that alone means nothing. I queried the number through dozens of online search tools which only revealed “Los Angeles, CA” as the subscriber information. This confirmed my suspicion that this was a VOIP number which was not assigned to a cellular account. I logged in to a free trial account at Twilio, opened the dashboard, clicked “Lookup”, selected the “name” and “carrier” options, and conducted a search. The result identified the VOIP provider as “go-text.me”. This site, located at <https://go-text.me>, confirms the number to be associated with a mobile app which allows “Unlimited texts and calls to the US & Canada from your own real phone number”. These numbers are commonly used to harass victims without disclosing a true identity. I now knew the service, but had no details to identify the suspect.

Next, I wanted to determine the way that the suspect accessed her photos. I confirmed that she synchronized all of her iPhone content to iCloud, including photos. I had her log in to her Apple account through a web browser and click on the Devices option. This displayed only her iPhone and MacBook laptop. This eliminated the possibility of another device associated with her account. However, it does not disclose access to her iCloud via web browser. While logged in to her iCloud account, I had her click on the “Sign out of all browsers” option and change her password to something randomly generated by a password manager. Next, I had her conduct a search within the email account associated with her Apple ID for “Apple ID was used to sign in”. This revealed a message in her spam folder announcing that someone had successfully accessed her iCloud account which included the date, time, time zone of the

user, and browser details. She confirmed that she has never accessed her account from a browser.

I now knew that someone had accessed her account at a specific time, and could make assumptions about the activity within her account. He likely already downloaded all of her photos, contacts, email, and other details. A quick search of her email address within my own data breach collection identified two commonly used passwords. She confirmed that one of them was her previous Apple ID password. I now assumed that the suspect found her email address online, identified a known password within a public breach, accessed her iCloud account using those details, identified her telephone number via her Apple account, downloaded all of her content, and then began the extortion attempt.

The suspect continued threatening her via text message and became more aggressive as she ignored the communication. She seemed willing to pay money to the hacker, but I always discourage that. I have hesitantly assisted ransom payments for clients, but the outcome was always the same. Even after the suspect received payment, he or she went ahead and published the content. There is no honor among thieves. I explained that there was a very good chance that these images would be published online regardless of meeting any demands, and there was little to nothing she could do at this time. If she paid the extortion, the attacker would keep the images and probably post them later. It would also make her a bigger target. If she paid once, she would likely pay again. Paying into ransom and extortion demands is never a solution, it is usually the beginning of a bigger problem.

The next morning, she woke to find a slew of text messages from the suspect. Although her 24 hours had not expired, he began posting content to the internet. This confirmed my assumption that he would publish content regardless of payment. One of the messages contained a link to a page on Pornhub.com. The page presented a video which cycled through her stolen sensitive images. Her name was present within the title of the video, similar to "Mary Doe naked and exposed". She was devastated to say the least. His text messages indicated that he had not sent this link to anyone yet, but demanded immediate payment in order to keep it private. He sent her a list of all contacts from her phone, which had been previously synchronized to her iCloud account. He informed her that she had two hours to send the Bitcoin or else all of these contacts would receive this link.

Mary and I discussed the options. She said that she could raise the \$50,000, but it would take some time and would cause financial strain. I again informed her that paying the ransom would not eliminate the potential of public exposure. The premature posting of images and childish language convinced me this was an immature young adult who simply knew enough about internet security to be dangerous. I discouraged any payment and convinced her to focus on damage control.

During our conversation, the suspect began sending the link to various members of her immediate family. Again, he was dishonoring his own deadline for payment. He sent the messages to the email addresses of her mother and brothers from a ProtonMail address in her name, similar to therealmarydoe@protonmail.com. The messages included the text of “Hey, check out my new promo pics for my next movie!” and a link to the pornographic images. While Mary began contacting her family in order to warn them about the abuse, I focused on removing the content from Pornhub.

Fortunately, removing content from porn sites is extremely easy. Most of them immediately remove the requested URLs and perform a manual review afterward. I submitted a request through the Pornhub removal page and cited the following reasons.

“Revenge porn, blackmail, & intimidation through a video published without authorization.”

Almost immediately after the submission, the Pornhub link began forwarding to an error page. The content was no longer available, for now. I know from experience that this suspect was not likely to go away, and he would probably become more aggressive. However, the messages currently waiting in people’s inboxes would not expose my client. We did not respond at all to his messages, and waited for his next move, which came about an hour after his previous contact. He sent Mary a new link to an online blog hosted on a free WordPress profile. This page contained three of the pornographic images of Mary, but the pictures were somewhat sanitized with small black bars covering vital areas to prevent them from technically portraying pornography. I had never seen this modification step before.

I immediately submitted a removal request to the appropriate page on the WordPress platform. I cited the Digital Millennium Copyright Act (DMCA) since Mary owned these images and WordPress may not deem them to be pornography. Within an hour, I received the following response from WordPress.

“We have reviewed your DMCA notice and the material you claim to be infringing. However, because we believe this to be fair use of the material, we will not be removing it at this time. Please note that Section 107 of the copyright law identifies various purposes for which the reproduction of a particular work may be considered fair, such as criticism, comment, news reporting, teaching, scholarship, and research. You are required to give consideration to whether a use of material is fair before submitting a takedown notification, as a result of the decision in *Lenz v. Universal*. Please note that you may be liable for damages if you “knowingly materially misrepresent” your copyrights – and we may seek to collect those damages.”

Not only did WordPress refuse to remove this inappropriate content, they threatened to seek financial damages from me for submitting a removal request, as I briefly explained within a previous chapter. I was shocked and quite angry. I submitted a second submission, but avoided

the DMCA process. Instead, I navigated to the abuse reporting site at <https://wordpress.com/abuse>. I chose the option of “This content contains my private information” and provided the URL of the exposure. WordPress notified me that the company does not believe “Photos of people”, “Publicly available physical addresses, email addresses, or phone numbers”, or “Names” to be private information. In the box designated for further information, I entered the following.

“Nude photos on this page depict a person (me) who was a minor. Child pornography is defined as nude photos of a person under the age of eighteen. Please remove these illegal images immediately.”

Hold your hate mail. First, my client is an adult in her 20’s. The nude images depicted what appears to be a young woman in her late teens or early twenties. Second, I found it unacceptable that WordPress would defend this type of extortion behavior. Finally, I said nothing untrue. The page does contain nude photos. My client was a minor at one time, just not now. Child pornography is illegal. These images are illegal as they were stolen as part of an online intrusion and extortion attempt. Notice I did not state that the images posted were child pornography. Within an hour after submission, the page was removed. You may disagree with my strategy, and I do not recommend that you replicate any of this without legal counsel, but the ultimate goal was reached. The inappropriate content being abused was removed.

The suspect was irate. He did not know with certainty that we had removed the page, but he knew it was gone. His response to our cat-and-mouse game took things to another level. He purchased a domain name and hosting account in order to continue publication of the nude photos. He then forwarded the new web page address to the same contacts as the previous attempts.

This presents the most difficult type of content to remove. Since this is a personal website, I cannot submit a request to the host, such as Pornhub or WordPress. Obviously, a removal request to the suspect would be pointless. The suspect had enabled privacy protection which hides the identity of the owner, which was likely false information anyway. A query of the domain, which was similar to marydoeexposed.com, identified the web host, which offered the first month of service for less than \$1.00. From the host’s website, I identified the appropriate abuse contacts. I sent the following email to the abuse team.

“The website located at marydoeexposed.com contains nude images of me which were stolen from my iCloud account. Distribution of these images through your servers is a violation of copyright laws and subject to civil litigation. I demand that these images are removed immediately.”

The entire account was suspended within hours. Mary and I both knew that this game could go on forever. We agreed it was time to step up the investigation into the identity of the suspect. Mary filed a police report with her local police department while I began digging. While I have witnessed some law enforcement agencies take immediate action, the reality is that their resources are limited. If a local department does not possess officers trained in cyber investigations, they simply do not have the tools or knowledge required to tackle these sensitive investigations. Most departments refer victims to the FBI, which has its own complications. It can take weeks or months for a federal investigation to be approved and launched. While I am happy to cooperate with any law enforcement willing to assist, my priority is to remove content for my client in order to minimize exposure as quickly as possible. Filing the report was only a formality. It notified law enforcement of the incident and allowed them an opportunity to investigate. When I am criticized later during an investigation, which happens often, I can prove that I made an attempt to bring law enforcement into the case. However, I do not wait for them.

I began reviewing all of the online evidence I had captured before removal. This included screen captures of all pages and content. The Pornhub username for the original publication was similar to “ihackcelebs4fun”. I began researching this username which mostly forwarded to other Pornhub pages identifying previous victims. However, I located several posts on Reddit from a person with the same moniker. The post matched the activity of posting stolen photos. I decided it was time to initiate contact. I located a Pornhub video which the suspect had posted a month prior to my client’s content. I sent a direct message from a covert Reddit account to the suspect’s Reddit username and referenced the older video, which was still online. I told him that I had a ton of similar images and asked if he was up for a trade. I offered to send content first so that he knew I was not trying to rip him off. This message was sent at noon on a Sunday, and I had heard nothing back by the end of the day. I assumed this was a dormant account and my message would go ignored.

While I was doing this on Reddit, Mary sent a response via text message to the suspect. She stated that she was working on getting money into Bitcoin, but assured that she had the funding. She insisted that he post no further images, and that she would refuse to send the funds if he did. He agreed to wait until the following day, which bought us some time. There was no intent to send any money. This was simply a ruse to stop the posting game and allow me to focus on the investigation.

At my direction, Mary sent a text message stating, “I tried to pay BTC to the address you gave me but it said bad address. I don’t know what to do”. The suspect became frustrated, but this is common in extortion. Telling people who are unfamiliar with Bitcoin to send large sums of digital currency is almost always met with problems. He asked which company she used, and she stated, “Coinbase”, which is a popular Bitcoin exchange. He asked her about the error message and she played dumb. He then gave her a command for which I was waiting. He

texted, “Send me a screen capture of the error”. This excited me because he was opening an opportunity for me to send some bait. I advise Mary to respond, “It says file to large. What is your email? I can send it there”.

I was not expecting him to share a personal email account in his real name, but communicating over email can have great advantages. My goal was to send him an image which included embedded tracking software which would disclose his IP address, computer details, and possibly approximate location. Once he disclosed his covert ProtonMail address, I took over all communication. I sent an email from an account through Gmail which I had created in Mary’s name. It included a link to an image which I knew would appear as a Photo-shopped file depicting a Coinbase account with a \$50,000 balance. The content was not important, but I hoped it would get him excited. Instead, I was counting on him clicking the link without much investigation.

The link was generated by a service called **Canary Tokens** (canarytokens.org). It allows me to send a URL displaying any image desired. When a target clicks the link of the image and views the content, a small script attempts to gather the information about his computer and connection as mentioned previously. This is always a gamble. Tech-savvy people know to look for this and will likely block the attempt. After analyzing all of his communication, he seemed like an anxious person just looking for a quick payday. Within a few moments after sending the link, I received a notification from Canary Tokens that the bait was taken.

The report stated that the offender was on an iPhone and disclosed the IP address of the connection. I had hoped that sending an email instead of text message would encourage him to check from his laptop, but this failed. After a quick search, I determined that the IP address was assigned to a VPN company, and was practically useless. This was also a failure. We were getting closer to him, but were far away from discovering an identity. The suspect responded via text telling Mary to try the payment again. Mary said that she will keep trying if he promised to stop uploading content. He agreed and we closed our investigation for the day. Mary ended the conversation with, “I can get this done first thing tomorrow”.

I woke up Monday morning to find an alert of a pending message within my covert Reddit account. The message, from the same username as the suspect Pornhub account, confirmed he would be interested in trading stolen photos. The previous attempt to obtain his IP address through a trap embedded into an image failed, but I found no harm in trying again. This was a different platform and a new day. I created a new infected image and sent it to his Reddit username. I sent a poor quality still capture from a publicly available pornographic video. This was a grey area, as I did not own the image or have authority to distribute it. However, I feel the intent justified the risk. Within seconds, I received a response within the Canary Tokens website. This time, the IP address was not associated with a VPN and the link was not opened

from a mobile device. Instead, the IP address was assigned to a national chain of banks and the computer used was a Windows 10 desktop with the Chrome browser.

I did not want to get my hopes up. While my suspect could be an employee of this bank, he could also be someone using public Wi-Fi at the business, a criminal connecting through a compromised on-site computer, or any other type of proxied association. My research into this bank indicated there were numerous buildings within the metropolitan area of the IP address block. This was a lead too big to ignore, but it would not be easy to isolate a specific offender.

I set my sights on the possibility that my suspect was a bank employee. Banks typically do not offer free Wi-Fi due to security reasons. Checking a Reddit message through a compromised business computer seemed to be a stretch. My hopes were that my offender was just sloppy. I identified the Chief Security Officer for this national chain of banks and contacted his office via telephone. After a few hops, I was connected to his secretary. I calmly and politely explained the situation without providing too many details, and made it very clear that an employee of this bank was using corporate assets during work hours to commit extortion. She seemed to take things seriously and promised to have someone contact me soon. An hour later, I received a call from an attorney representing the bank.

The call was awkward to say the least. It was obvious that the attorney did not want to implicate the bank in any way or acknowledge an internal issue. At one point, he asked, "What are you asking us to do?", which I eagerly answered. I clearly explained that my only goal was to protect my famous client. I had no desire to smear the name of the bank or go public with this information. If the bank was willing to cooperate in identifying the employee responsible for this situation, I was willing to keep it quiet. If the bank refused to cooperate, I was willing to take my evidence to the local police, which would make the entire scandal public information. I expressed my opinion that we both had much to gain by keeping this investigation as quiet as possible.

The attorney quickly ended the call and refused any further contact attempts from me. Lesson learned. Much like my job is to protect my client, corporations only look out for their own best interests. This was a failure. Fortunately, I did not disclose any details which would help them identify the suspect and compromise our own investigation. I went back to the drawing board.

While I was contacting the bank, Mary was receiving additional messages from the suspect. He told her that time was up and either she must pay or he would publish all of her photos directly to her contacts and send copies to various tabloids. He further threatened to create a torrent file which could be seeded in a way which could never be removed. It seemed that we

had stretched his patience. I had yet to hear back from any law enforcement personnel about the possibility of opening an investigation.

I revisited his online presence. I read through every post he had made on Reddit. In retrospect, I should have started there before trying to get his IP address. His post history seemed redacted. There were posts which had been deleted and some which appeared to have modified text. I replicated my search of his posts on a third-party archive called **Pushshift** (pushshift.io). I generated a custom URL which would display all posts made by him as they were archived soon after publication. The exact URL for this example username appeared as follows.

api.pushshift.io/reddit/search/comment/?author=ihackcelebs4fun&sort=asc&size=1000

The result was over 200 posts made by the suspect over the past two years. This presented much more content than I found on his live profile. I began devouring posts for any further clues. Within this treasure, I found posts about banking, which fit the employment at the bank identified in the IP address. I also found numerous posts within the Pomona, California Subreddit (reddit.com/r/Pomona), which was within the geographical area of the IP address. I was getting closer. The gold prize was the following deleted message.

2019 Acura TLX Tech Trim in like-new condition. 3457 miles. No damage.

<https://imgur.com/a/XaOj4rC>

The Imgur link displayed several photos of a vehicle, and the post was recent (2019). None of the images displayed a license plate, but this was my next solid lead. I replicated the search of “2019 Acura TLX Tech Trim” on Craigslist and received the following post.

2019 Acura TLX Tech Trim in like-new condition. 3457 miles. No damage. Call Matt at (909) [REDACTED].

The post included the full telephone number and the same photos as linked from the Reddit post. I now knew his name was potentially Matt, he might work at a specific bank in the area of Pomona, California, and he might own a 2019 Acura. I replicated my search on Twilio of this number which provided a potential last name. I searched this name on LinkedIn, but received no results. I eventually found a person with this name from Pomona on Twitter. However, there was no direct connection from that account to my suspect. I presented all of my information to Mary, and proposed one last desperate attempt.

Since time was not on our side, and we expected the suspect to blast her details to all of her personal and work contacts, I proposed we call him out. Tell him what we “know” about him

and hope it is right. If we are wrong, it may make him laugh and go crazy online. If we are right, it may scare him. In my mind, we had nothing to lose. I was confident the suspect planned on publishing her photos regardless of payment. She agreed with my plan, and I sent the following email to the ProtonMail address received earlier. I placed [REDACTED] in place of the actual details which I disclosed to him.

"Hi Matt,

I am assisting Mary Doe with the investigation into your extortion attempts. My final report has identified you as Matt [REDACTED]. You work at the [REDACTED] branch of [REDACTED] Bank. You drive a 2019 Acura which you are having trouble selling. I have evidence that you have used computers owned by your employer as part of this crime. Since these are bank assets associated with a corporation covered under FDIC rules and laws, there are substantial federal offenses for which you can be charged. Mary and I are still determining our next actions. For now, we are demanding you to cease all distribution of content while destroying all related data. In return, we will consider keeping our evidence to ourselves. If we receive no response from you, we will forward this content to your supervisor, [REDACTED], as well as Detective [REDACTED] at the Pomona Police Department. Extortion sucks, eh? You can respond here or contact me directly at [REDACTED]."

This is where I want to tell you that he was scared. I want to close this chapter with a victory and messages from the suspect pleading with us to show mercy toward him. That would be untrue. He did not respond to me at all. Instead, he released all of the images as promised and sent links via email to every contact on my client's phone. Mary was officially exposed to the world.

You may believe I reacted foolishly. You are right. It was a desperate attempt, and it failed. It expedited us into the position in which we would have likely found ourselves, even if we had cooperated and given money. I began removing the online content he published, which was fairly successful. He simply replicated his methods of publication from earlier, and I reactively tackled each exposure. He never posted a torrent file, but the damage was heavy. Numerous friends, family members, associates, co-workers, and business interests of Mary viewed the sensitive photos. All of them will say this event had no impact on their relationship with Mary, but I don't believe that. Today, all of the content has been removed.

A few days after the final exposure, a detective from Mary's local police department announced she would be opening an investigation. I made full disclosure of my actions, and accepted all responsibility for the outcome. I was chastised for a few minutes, but we then began strategizing about the next steps. The detective was very sharp, but had no experience with computer crimes. However, she had something more powerful. The detective could request court orders.

She first targeted Pornhub for information about the uploader, but they are a Canadian company. Her U.S. court orders would be of little help. She then reached out to a liaison with the Royal Canadian Mounted Police (RCMP), and they agreed to create a Canadian order on her behalf. This is quite common in law enforcement. While she waited, she issued a court order to Reddit demanding information on the target account. Reddit confirmed the user's IP addresses and Gmail address provided during creation. A court order to Google confirmed the identity of the suspect. A warrant was issued and he was arrested.

I am intentionally leaving out some of the details at the request of the detective who worked the case. However, I can disclose where I was wrong. My fatal mistake was assuming the vehicle posted on Reddit belonged to my suspect. It did not. In fact, we have no idea why he posted those images. Getting this wrong led me to disclose a name to the suspect of which he had likely never known. My education from this is that any suspect can really throw off an investigator by posting a vehicle for sale which has no connection to him. The suspect did work for the bank, but not at any local branch. Enough of my email was wrong that he felt confident releasing all of the photos. A search warrant for his laptop, which had been seized during his arrest, indicated that this was the seventh incident of attempted extortion. Five, including my client, never paid. Two paid the full amount requested. All seven victims had their photos released publicly. Because of this, I don't have regret in my actions. It was a lose-lose situation. However, I now handle these extremely differently.

I tell all of my clients, regardless of the situation, absolutely cease all communication with the suspect. There is nothing to gain. Furthermore, no response to the extortion at all has been the most successful strategy I have found. If you ever receive an extortion attempt, I encourage you to completely ignore the demands. Paying the ransom usually results in published data anyway. Responses confirm that the suspect has your attention. Notify law enforcement, and hope that your local agency has the resources to investigate.

After this event, Mary obtained all new hardware, online accounts, mobile plans, and alias profiles as explained throughout this book. The Apple account was completely deleted. The suspect was charged with several counts of extortion, released after posting bail, and is awaiting trial during the writing of this chapter. Neither Mary nor I have seen or spoken to him and he has made no attempt to contact either of us. I watch the case closely, and I will be present when Mary testifies.

I want to close this chapter with some lessons learned which may help readers digest the recommendations presented toward the beginning of the book. My focus here is to simply present the methods which could have prevented the entire mess. Please know that I am not blaming Mary. I have executed very similar digital blunders toward my own profiles before I jumped into the privacy and security game. Ten years from now, I might be disgusted with my current strategies presented here. Hindsight is always 20/20. Treat all mistakes as an education.

- Mary's Apple account was in her real name and associated with a mobile device serviced in her name. Ideally, Apple (or Google) should never know your true identity. This way, social engineering attacks toward Apple are very difficult. If a suspect does not know the name you used to create an account, abuse of telephone, email, and in-store support should be quite difficult.
- Mary's email address to access her Apple account was a publicly identifiable personal address. Most of us have at least one email address which is publicly associated to our name through online people search sites, data breaches, or social networks. The email address connected to an Apple ID or Google account should always be a unique dedicated generic address. It should not be used anywhere else. This prevents attempted password resets and login attempts.
- Mary recycled a password from another online service to her Apple account. I have done this before, but I was lucky to avoid any compromised accounts. Every password should be unique for each service. Password managers can generate random options and store them for easy usage.
- Mary's iPhone was configured to enable iCloud synchronization, which is the default option. This copied her contacts, photos, videos, documents, and other details onto Apple's servers. Once the suspect accessed her account, he had his own copy of her data. I insist that any mobile Apple device is never allowed to access iCloud. I also check the online iCloud account associated with an Apple ID on occasion in order to verify that no data is present.
- Mary allowed her mobile device to be the primary storage of personal photos and contacts. Even if she had disabled iCloud, it could have been re-enabled after a major software update. Because of this, we should never store contacts in the default device address book, nor photos on the device's internal storage. Instead, store all contact details within ProtonMail and copy and paste from there when needed. Photos and videos should be occasionally moved to secure storage within a VeraCrypt container and removed from the mobile device.
- The telephone number associated with the Apple ID was Mary's true cellular account. This allowed the suspect to initiate conversation through her native messaging application. If he had attempted a SIM swap or malware attack, he could have had success. If Mary had provided Apple a VOIP number, any attempted attacks would have been minimized. Avoid giving Apple ID (or Google) accounts any number when possible by signing up through their website (instead of from the device). Apple still knows the cell number assigned to the device, but it would not be visible to the suspect within the iCloud account.

Today, Mary has exceptional digital operational security. Occasionally, she forwards ideas which I had never considered. The entire GrapheneOS section within Chapter Two contains heavy input from her, as she has completely moved on from Apple devices.

Failures

There are plenty more failures that could fill twice the pages currently in this book, such as the following, which all happened to me over the past five years.

I worked with a CEO dealing with death threats, staying at a hotel under an alias, but attending a convention next door under his real name. It did not take long for his adversary to find him and his room using the methods discussed previously. Surprisingly, the suspect did not confront my client, but his restaurant bills were enormous thanks to the culprit's taste for expensive steaks (all billed to my client's room). The intruder creepily stalked my client from a short distance, and I had no clue. At one point he introduced himself to the client's daughter at the hotel pool. I learned about this after the event. This was the last time I tried to run counter-surveillance for a client. I now hire professionals to do the job right.

I assisted a victim of extreme physical abuse received from her husband. She was hospitalized due to his violence. Her mother hired me to remove her from the hospital and take her somewhere safe and away from him. The husband was always by her side to make sure she did not talk with the police. When I saw an opening, I executed my version of an extraction. I tried exiting with the victim in a hospital gown through a fire escape, and hospital security detained me until police arrived. I was questioned for over an hour. Not my best execution.

Another domestic violence victim contacted me desperate for assistance leaving her abusive situation. She had no money, and a relocation would not be cheap. I was working with a celebrity at the time on an unrelated matter and spoke generically about the situation she was in. He insisted on paying her costs and she was safely relocated under a new alias using the techniques discussed here. She insisted on meeting him to thank him. He wanted to meet her as well. With both clients' consent, I arranged a secure communications channel which either of them could destroy if desired. They hit it off. Too well. She was photographed having lunch with him in Los Angeles, and the photo was published in a tabloid. My job was to create a private world for the client, not place her photo in a magazine. This was a valuable education.

In early 2019, one of my clients received a text message with an attached photo. It was a selfie from her former lover displaying luggage and an airline ticket to the airport near her "anonymous" home. She had been hiding from him after suffering years of physical abuse. Somehow, he had discovered the city she was in, and he appeared determined to come find her. I needed to buy some time, so I turned the tables on him. I could see the airline carrier from the ticket and the departure and arrival details. Out of desperation, I began sending him text messages stating that his flight had a three-hour delay. He bought it and stayed at home while continuing to send her text messages. He arrived at the airport an hour after his flight had left and discovered there was no delay. He missed his flight. I still receive hate mail from him after the client bragged to him about my services (Hi Jerry).

I have been on the receiving end of a felony stop after a stalking suspect called the police and reported me as a kidnapper. I was once declined nomad enrollment on behalf of a client on a late Friday afternoon due to missing paperwork, requiring us both to stay in town until Monday. Once, while impersonating a client during an email attempt to remove online information, I was asked “Is this Michael Bazzell?” by the customer support for the service. While these situations were all quite embarrassing, they were also educational. I will never forget the mistakes I made which led to these failures, and I will never repeat them.

I have also made mistakes in reference to my own privacy strategies. Years ago, I initiated a contract for a new personal home and provided earnest money to the title company from a trust. After everything was accepted and both parties agreed to all contingencies, I had to back out. While visiting the home on several occasions, I realized I had my work phone with me, actively connecting to cell towers. I slipped and took a business call in front of the listing agent. She heard enough of the conversation to know my unique business details. Worse, I made an initial call to the power company from a VOIP number associated with my real name, which was likely added to the profile for this address. It is very possible none of this would have compromised my privacy publicly. I couldn’t take that chance. I likely overreacted out of paranoia fueled by my past. The lost earnest money was the expense for that education. I was ready to do it right the next time.

I disclose all of this to stress one important final thought. Achieving extreme privacy is an art. Books full of tutorials such as this lay a good foundation for achieving a level of privacy appropriate for your situation. However, no book will provide everything you need to live a completely invisible life or create a new life for others. My best education has been through experiences and failures. My failure rate at various tasks was very high early in this game. I have been denied utilities in an alias name on behalf of clients more than I have been granted anonymous accounts. I happily admit that I have failed more than I have succeeded, but that ratio becomes lower every year which goes by. In the past year, I have had a 99% success rate with achieving anonymous homes for clients. It took time to develop the proper execution of each technique. Experience will go further for you than any written text. I hope something in this book helps you achieve your privacy goals.

There are many other less-than-ideal scenarios which I can never disclose publicly. I will only say that I am honored to have been trusted by so many clients over the past several years. This has created friendships with amazing people, all of which are bonded by the secrets which we have all sworn to keep private. Because of these promises, I have reached the end of the details authorized for publication by my clients. I sincerely thank all of them who allowed me to provide an insight into the need for privacy and security.

CONCLUSION

I truly hope you never need the strategies discussed here. The best-case scenario is that you had an interesting read about the lengths some people go through to protect their privacy. As stated in the beginning, there will be no time to fix things if something bad happens. Extreme privacy is not reactive. It only works when you proactively protect every level of your own exposure. This requires a lot of effort. However, once everything is in place, you can experience the comfort of knowing you possess a private home for you and your family, secure digital habits, and the knowledge to create a private bubble whenever needed. If any negative incidents come your way, you have a safe retreat which no one knows about. Journalists, private investigators, enemies, and criminals will have no way of finding you. Stay safe, and stay private.

If you have adopted the strategies within this book, congratulations. You are sitting in your anonymous home with no affiliation to your name. The car in your garage possesses license plates which cannot publicly be tracked back to you. You have a ghost address, and appear to be a normal person on paper. You have never been to your “official” address on file. You have trusts and LLCs executed and ready to be used for privacy protection. You possess anonymous payment sources and can tackle daily purchases without exposing yourself. Your email accounts are private and secure, and everything in your digital life possesses unique and randomly generated passwords. You have an extremely hardened life, and will be a very difficult target if anyone should come after you. You are practically invisible.

If you would like to stay updated in reference to the latest privacy, digital security, and online investigation strategies which I teach, please visit inteltechniques.com. On this site, you can access my weekly podcast, blog, and contact information for live events, plus information about my privacy-related services and personal consultations. Thank you for reading. I wish you the best in your privacy adventure.

MB

- Address Disinformation, 501
Alias Name, 324
Alias Wallets, 380
Amazon, 396
AnonAddy, 132
Anonymous Payments, 363
Antivirus, 15, 19
Apple ID, 18, 41
Appliance Purchases, 405
Authy, 103
Auto Supply Stores, 313
Background Services, 538
Backups, 16, 81, 112, 175
Bank Accounts, 437
Beryl Router, 202
Birth Considerations, 463
Birth Tourism, 484
Bitcoin, 418
Bitwarden, 101
Bleachbit, 15, 28
Bluetooth Tracking, 92
Brew, 19
Business Disinformation, 512
Business Registration, 433
Calendars, 144
Camera Blocking, 89
Carbon Copy Cloner, 24
CCPA, 540
Cellular Service, 47
Census, 542
Checks, 373
Children, 354
ClamAV, 19
Cloudflare, 122
CMRA, 211
Computers, 11
Connected Devices, 489
Contact Information, 519
Contacts, 144
COVID-19, 567
Credit Card Processing, 438
Credit Cards, 374, 379
Credit Fraud Alerts, 561
Credit Freeze, 555, 557
Credit Opt-Out, 556
Credit Report, 555
Criminal Information, 553
CTemplar, 143
Customer Support, 417
Data Removal, 520, 543
Death Considerations, 466
Death Disinformation, 514
Decoy Phone, 93
Disinformation, 498
DMCA, 547
DNA Kits, 494
DNS, 122
Doxing, 518
Driver's License, 222
Drones, 585
Dual Citizenship, 475
EIN, 437
Electrum, 418
Email, 127
 Alias Email, 129
 Business Email, 138
 Custom Domain Email, 134
 Email Archives, 139
 Email Forwarding, 131
 Email Privacy, 142
 Encrypted Email, 128
 Masked Email, 132
 ProtonMail, 128
Employment, 425
 Employee ID, 428
 Parking Permits, 430
 Self-Employment, 432
 Traditional Employment, 426
Faraday Bag, 84
Faraday Wallets, 583
Fastmail, 138
File Sharing, 156
FileVault, 18
Financial Data, 496, 548
Firearms, 584
Firefox, 115
Firewall, 87, 177
 Android Firewall, 88
 iOS Firewall, 87
Fitness Trackers, 495
Florida Domicile, 227
Ghost Addresses, 211
Gold Coins, 421
Google Voice, 65, 68
GrapheneOS, 35
Haven, 333
Health Insurance, 228
Hidden Cameras, 331
HIPPA, 410
Home Purchase, 337, 345, 349
 Home Choice, 343
 Home Privacy, 573
 Home Sale, 360
 Home Search, 338
 Home Security, 576
Home Network, 177
Hotels, 319
ID Scanning, 381
Insurance, 303, 383
Internet Hotspots, 394
Internet Service, 390
iOS, 41
iPod Touch, 82
KeePassXC, 98, 147
Kindle, 492
KnockKnock, 21
Legal Infrastructure, 231
Libelous Websites, 549
License Plate Readers, 309
Linphone, 49
Linux, 12
Linux Phones, 88
Little Snitch, 21
Living Will, 468
LLCs, 255
 Articles of Organization, 258
 Certificate of Organization, 260
 New Mexico, 257
 South Dakota, 271
LocalCDN, 120
Lockdown, 87
Lodging, 319
LuLu, 23
macOS, 18
Mailing Lists, 539
Marriage Considerations, 461
Masked Debit Cards, 368
Mat2, 142
Medical Services, 408
Metadata, 142
Microphone Blocking, 89

- Mobile Devices, 33
 Tracking, 567
- Moving Services, 403
- Multi-Account Containers, 119
- MySudo, 64
- Name Change, 459
- Name Disinformation, 499
- Neighbors, 355
- NetGuard, 88
- Nomad Life, 456
- Nomad Residency, 219
- Notes, 153
- Number Forwarding, 68
- Number Porting, 65
- OnlyKey, 109
- Onyx, 24
- OverSight, 23
- Pagers, 94
- Parking Permits, 430
- Password Managers, 98
- Passwords, 97
- Personal Websites, 508
- Pets, 445
- pfBlockerNG, 197
- pfSense, 179
- Photos, 543
- Physical Privacy & Security, 573
- PMB, 213, 219
- PO Box, 211
- Portable Routers, 202
- Prepaid Cards, 365
- Privacy.com, 368
- Protectli Vault, 178
- Proton Drive, 156
- ProtonMail, 138
- ProtonVPN, 79, 123
- Radio Frequency Monitoring, 344
- Remote Work, 569
- Rental Homes, 329
- Revenge Pornography, 545
- Reward Programs, 327
- Right to be Forgotten, 554
- RSS Feeds, 172
- Search Engine Indexing, 537
- Secondary Device, 82
- Secure Messaging, 74
- Self-Employment, 432
- Signal, 75, 153
- SimpleLogin, 132
- Slate Router, 202
- Sole Proprietorship, 436
- South Dakota Domicile, 219
- Standard Notes, 153
- Storage, 112
- Store Memberships, 411
- System Cleaner, 15
- TAILS, 170
- Task Explorer, 21
- Telephone Disinformation, 509
- Telnyx, 61, 152
- Temporary Housing, 319
- Texas Domicile, 227
- Thunderbird, 139, 172
- Tolls, 307
- Tor Browser, 155
- Travel Security, 582
- Traveling, 157
- Tresorit, 156
- Trusts, 231
- Amendment to Trust, 248
- Certification of Trust, 250
- Living Trust, 232
- Traditional Trust, 240
- Trustee, 247, 254
- Tutanota, 143
- Twilio, 50, 152
- Two-Factor Authentication, 103
- uBlock Origin, 117
- Ubuntu, 12
- USB Operating Systems, 170
- Utilities, 388
- Vaccines, 570
- Vehicles, 275
- Choice, 304
- Insurance, 303, 318
- LLC Purchase, 292
- Loans, 304
- Markings, 305
- Privacy, 312
- Registration, 276
- Services, 306
- Tracking, 315
- Trusts, 276
- VeraCrypt, 26, 112
- Verification Questions, 564
- Videos, 544
- Virtual Currencies, 418, 438
- Virtual Machines, 162
- Clones, 167
- Exports, 167
- Snapshots, 156
- Troubleshooting, 168
- Usage, 169
- VirtualBox, 24, 162
- VOIP, 49, 152
- VOIP Issues, 73
- Voting, 226
- VPN, 79, 123, 177
- Web Browsers, 115
- Wi-Fi Tracking, 92
- Wills, 470
- Windows, 25
- Wire, 77, 153
- Wireless Routers, 199
- YubiKey, 103, 106