Hiding From The Internet

Eliminating Personal Online Information

Third Edition



Michael Bazzell

Hiding from the Internet

Eliminating Personal Online Information

Third Edition

Michael Bazzell

Hiding from the Internet:
Eliminating Personal Online Information
Third Edition

Copyright © 2016 by Michael Bazzell

All rights reserved. No part of this book may be reproduced in any form or by any electronic or mechanical means including information storage and retrieval systems without permission in writing from the author.

First Published: January 2016

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

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

ISBN 13: 978-1522914907
ISBN 10: 1522914900

Contents

About the Author

Introduction

CHAPTER 1: Self Pre-Assessment
- Search Engines
- Alternative Search Engines
- Search Tool
- Ancestry Records
- Email Addresses
- User Names
- Location Based Searches

CHAPTER 2: Self-Background Check
- Public Websites
- People Directories
- Telephone and Address
- Social Networks
- Facebook
- Private Databases
- Credit Reports
- Personal Reports

CHAPTER 3: Preparation
- Loyalty Programs
- Utility Bills
- Removal vs. Disinformation
- Anonymous Email Addresses
- Anonymous Telephone Numbers
- Mailing Address

Custom Opt-Out Request Forms
Anonymous Fax Service

CHAPTER 4: Online Protection
Basic Protection
Antivirus
System Updates
Anti-Malware
System Cleaner
Alternative Browser
Firefox Extensions
Intermediate Protection
NoScript
Search Engines Settings
Advance Protection
VPN
Tor
Tails Boot CD
Virtual Machines

CHAPTER 5: Credit Companies
Credit Opt-Out
Fraud Alert
Credit Freeze
Credit Options
Secondary Credit Card
Prepaid Credit Cards
Masked Credit Cards

CHAPTER 6: Anonymous Purchases
Online Purchases
Amazon
Kindle
Ebay and PayPal
Store Purchases
Services
Packages

CHAPTER 7: Anonymous Telephones
- Contract Terms
- Choosing a Device
- Factory Restore
- Cellular Service
- VOIP Solutions
- Complete Reset
- Encrypted Communications
- Signal
- Silent Phone
- Wickr

CHAPTER 8: Personal Data Removal
- People & Telephone Search Engines
- Caller ID Databases
- Email Assumptions
- Public Data Brokers
- Non-Public Data Brokers
- Data Marketers
- DMA Choice
- Catalog Choice
- Ancestry Records
- Online Coupons
- Loyalty and Reward Cards

CHAPTER 9: Social Networks
- Privacy Settings
- Content Removal
- Delete Accounts
- Facebook
- Twitter
- Google
- YouTube
- Google+
- Instagram
- MySpace
- LinkedIn
- Photos

Google Maps
Blogs

CHAPTER 10: Web Publishing
Domain Registration
Search Engine Control
Robots.txt File
Webmaster Tools

CHAPTER 11: Government Records
Property Tax Records
Data Removal
Ownership Change
Internal Revenue Service
Voter Registration
Court Records
Concealed Carry Permits

CHAPTER 12: Disinformation
Name Disinformation
Address Disinformation
Location Spoofing
Telephone Disinformation
General Tips

CHAPTER 13: Aliases
Choosing a Name
Email Addresses
Telephone Numbers
Employment
Hometown
Social Networks
Identification
Family History
Digital Footprint
Legalities

CHAPTER 14: Future Habits
- Identity Verification
- Telephone Calls
- Smart Devices
- Monitoring
- Website Analytics

CHAPTER 15: Major Life Events
- Purchasing a Home
- Renting a Home
- LLC Bank Accounts
- Anonymous Utilities
- Vehicle Purchases
- Marriage
- Divorce
- Death

CHAPTER 16: Data Leakage Response
- Home Information Leakage
- Photo Leakage
- Financial Information Leakage
- Reputation Information Leakage
- Criminal Information Leakage

CONCLUSION:

About the Author

Michael Bazzell

Michael Bazzell spent 18 years as a government computer crime investigator. During the majority of that time, he was assigned to the FBI’s Cyber Crimes Task Force where he focused on open source intelligence, hacking cases, and personal data removal methods. As an active investigator for multiple organizations, he has been involved in numerous high-tech criminal investigations including online child solicitation, child abduction, kidnapping, cold-case homicide, terrorist threats, and high level computer intrusions. He has trained thousands of individuals in the use of his investigative techniques and privacy control strategies.

Michael currently works and resides in Washington, D.C. He also serves as technical advisor for the television hacker drama "Mr. Robot" on the USA network. His books Open Source Intelligence Techniques and Hiding from the Internet have been best sellers in both the United States and Europe. They are used by several government agencies as training manuals for intelligence gathering and securing personal information.

Introduction

Hiding from the Internet

Many people believe that privacy is dead. In ***Open Source Intelligence Techniques*** I demonstrated how anyone can use the internet to locate personal information about oneself or others. From social networks to people search engines, it is simply too easy to find private information about each of us online. The internet will usually identify your residence, family members, telephone numbers, shopping habits, vehicles, employers, date of birth, education history, and many other details that should not be public. This book will help you maintain your privacy from the general public searching the internet.

Almost every online repository of personal information will allow you to remove your personal information. Since these companies make money from selling your private data, they do not make this removal process obvious. You will not see a website such as People Finders list a huge graphic on the top of their home page that says “remove your data here”. Instead, they bury these links to keep the majority of viewers away from online removal submissions and written removal request instructions. This book identifies the best effective ways to remove your personal information from public databases.

Third Edition

The first edition of ***Hiding from the Internet*** was released in August of 2012 followed by a second edition in 2014. Since then, a lot has changed. Many of the techniques for information removal were slightly different than the requirements today. Some of the companies simply stopped responding to removal requests. More importantly, numerous new online companies indiscreetly announce to the world all of your private information. In 2016, I am seeing single companies

create multiple copies of their databases across redundant websites. It is harder than ever to remove personal information from the internet.

This edition attempts to tackle these issues and provide new thoughts about how to effectively protect your personal details. Additionally, new chapters have been added to discuss completely anonymous cellular telephones, new aliases, private web publishing, data leakage response, and ways to keep up with the changes that will take place after this book is printed. The entire book has been re-structured to provide an orderly solution to protecting your privacy while presenting new ideas that have surfaced over the past two years. Approximately one-third of the book is recycled information, one-third is updated details, and one-third is completely new content. The first four chapters were extracted from the second edition with slight modifications, and still apply. Readers who have executed a previous edition may want to start on chapter five of this new edition.

Another big change is the way that I approach data removal from websites. In previous editions, I devoted numerous chapters to providing detailed instructions for every service. These steps would then change slightly, leaving this content a bit outdated. In this edition, I have provided one large chapter devoted to information removal. This chapter contains workbook style content designed to forward you to the best removal option. It is compressed into an orderly fashion that will make room for new overall techniques that will apply globally.

Why do you care?

The process of removing your personal information from the internet is not quick. It may take quite some time and may never be 100% complete. For some, it may not be worth the time. For many people though, it is worth every minute. The most common reasons for removing personal information usually fall into one of the following five categories.

Identity Theft Victims

Some sources estimate that one in every three Americans will be impacted by identity theft at some point in their lives. When I speak to groups, I usually poll

the audience and discover that at least 25% of the room has been a victim of this type of crime. Most people make it extremely easy for a criminal to obtain enough information from the internet about them to obtain identification and start a line of credit in the victim's name. Following the procedures in this book will make this process more difficult, causing the criminal to move on to someone else. I hate that we cannot stop all cybercrime, but I take comfort knowing that I can likely prevent it from happening to me.

Targeted Subjects

There are many professions that are often targeted for personal information such as law enforcement, federal agents, judges, attorneys, prosecutors, public officials, and other members of the government. These subjects should put extra effort into protecting their details from the general public. Law enforcement officers across the country have been doxed in the wake of incidents like those in Oakland, CA, Baltimore, MD, and Ferguson, MO. Prosecutors and judges have historically been targeted by sophisticated criminal enterprises and drug organizations. Members of the judicial system at all levels have been threatened by parolees. Members of our nation's criminal justice system should not wait until they face a personal threat to begin securing their lives.

Special Operations and the Intelligence Community

As a former government employee, I have a strong desire to keep my information private. Unfortunately, I no longer believe that I can rely on the government to protect my information. During the writing of this book, large breaches occurred against the Office of Personnel Management. This is the government entity that houses background checks and security clearances. I have held high-level clearances within the intelligence community. Personal information about me was stolen in this breach including my social security number, financial information, and sensitive family details. If you work in one of these communities, it is in your best interest to protect your own information before it is too late. This information may make you vulnerable overseas or compromise the safety of your family.

Celebrities, Executives, and the Wealthy

Celebrities, executives, and the extremely wealthy are common targets of stalking, extortion, scams, and sometimes physical violence. Members of malicious groups like Anonymous target individuals in this category. Paparazzi and journalists hound celebrities and executives. This book can help these individuals opt-out of the public view and recapture a private, personal life.

Dedicated Privacy Enthusiasts

This book is also for those who care enough about their privacy and security to pursue it, even though they do not fall into one of the aforementioned categories. Individuals in this category are much like me. They already understand the dangers to privacy and security and need no convincing. These individuals understand the risks to personal finances, reputations, and the safety of their families.

Regardless of which of these categories you fall into, the sooner you begin this process the bigger the benefits will be and the faster you will begin to see them. Even if you cannot do it all now, do what you can as soon as you can. It is also highly recommended that parents begin to implement these techniques on behalf of their minor children. How much easier would it be to demand your privacy back if most of the information available had never been put there in the first place?

Will this help you disappear?

Yes, and no. Eliminating your personal information from the internet will make it much more difficult for someone to locate you, but not impossible. As long as you have a house in your name, property taxes in your name, utilities in your name, or personal vehicles registered at your address, you can be found with legal action. Nothing in this book will hide you from the government. It will, however, stop the general public from obtaining your personal information. For those reading this that hope to use the techniques to hide from the IRS, pending litigation, active warrants, or paying child support, please move along. This book will do nothing for you. If you want to prevent nosey co-workers and sleazy criminals from finding out where you live, this book has you covered.

What will you need?

This book will provide all of the instruction that you will need to remove the personal information stored about you on the internet. A special page has been created on my website to help with the process. Navigate to **www.inteltechniques.com** and click the "Privacy" section. This page will have every link that is presented in this book, without the instruction. As links change, I will update this page to reflect the changes. As new services arrive, I will include new links to eliminate your data. The page is divided into sections for each chapter. You will also find related posts on my blog at this same location. This book will explain the methods of living a normal life, but one that is invisible on the internet. While the book is a one-stop-shop for your privacy, you must bring three things.

Initiative: There was a time when you could be a relatively private person by requesting that your landline phone number be unlisted. This is no longer the case. Privacy is no longer a passive process. A lack of participation in the digital world does not make you private. If you wish to be private, it is still possible to opt-out of the standard model, but you must be willing to pursue it, to make it happen yourself, and to demand it. This book merely provides the knowledge. You must have the willingness, determination, and discipline to make it happen.

Patience: Though I recommend that you start on this path as soon as possible, understand that you will not disappear overnight. I have experienced successes in finding ways to protect my privacy, and I have experienced significant failures when executing new techniques. There is much you can do right now to make yourself less visible and safer. Do not become discouraged if you find that you experience a setback.

Vigilance: Attaining your desired level of privacy and security is only the first step in a lifelong process. You will constantly be asked to give out your telephone number, email address, and even home address by parties that wish to market your information. You will also sometimes have to give out this information to take advantage of a product or service. To achieve and maintain your privacy, you must be prepared with alternate information that does not compromise your real information. After investing a great deal of time and

energy into reclaiming your privacy, you should guard it intensely.

Finally, I should very clearly state that I am not an attorney and this book contains no legal advice. Please consult with an attorney before attempting the advanced techniques outlined in this volume. This writing shares my experiences with executing basic and advanced methods for achieving complete privacy. Your results may vary. The entire content of this work was accurate to the best of my knowledge as of January 2016. Technology constantly evolves, and you may identify outdated content. Please refer to my website for any updates. Further, many of the educational theories of this work would require you to violate the terms of service of various online providers. On rare occasion, the government has claimed that violating a private agreement or corporate policy amounts to a Computer Fraud and Abuse Act (CFAA) violation. While I believe that this should not be the case, always proceed with caution and at your own risk.

Ready?

Whatever led you to this book, your interest in the topic indicates that you are ready to begin a journey into online personal information removal. Let’s get started.

Chapter One

Self Pre-Assessment

Before you embark on the adventure of removing your personal information from the internet, you should take a moment to identify the types of personal information present. Everyone will have different types of content visible about them. Each situation will require a unique strategy for removal. A person that owns a home and has a property tax record will find much more personal details online than a person that rents a home with included utilities. Also, a person with several social networks will see many more details than a person that has none. This chapter will help you quickly discover the amount of work that you will have ahead of you.

Search Engines

The first basic step is to identify the standard information available about you within search engines. In order to properly search your information, you will need to do much more than a standard Google search. Search engines will help you tremendously, but you will need to provide specific instruction when conducting your queries. For the first group of searches, assume that the following information describes you.

John Williams
1212 Main Street
Houston, TX 77089
713-555-1234

Searching “John Williams” will likely not be productive. Even if it were a unique name, the results would include spam and websites that provided no

valuable information. Instead, conduct the following searches including the quotation marks.

“John Williams” “77089”

This query instructs the search engine to locate web pages that have exactly John Williams and 77089 on the same page. This will eliminate many unwanted pages that do not contain relevant information. If your name is generic, such as John Williams, you may still be bombarded with unwanted results. Try the following search.

“John Williams” “1212 Main”

This query instructs the search engine to locate web pages that have exactly John Williams and 1212 Main on the same page. This will likely display pages that announce your home address to the world. These will be the pages that you will target for information removal. You should also search the following example to locate pages that display your home telephone number.

“John Williams” “555” “1234”

This query instructs the search engine to locate web pages that have exactly John Williams and 555 and 1234 on the same page. The two sets of numbers were searched separately in case the target websites did not use a hyphen (-) when separating the numbers.

If you live alone, these searches will likely suffice. However, your listing may be displayed in the name of your spouse, a parent, or roommate. Alter the searches to include any appropriate names. If you have a unique last name, such as mine, you could try the following searches to catch all family members.

“Bazzell” “1212 Main”
“Bazzell” “555” “1234”

These queries will locate online content that references you and your home.

Additional searches should be conducted based on your name and associations such as your employer, interests, or organizations. Create your own custom queries based on the following example searches.

"Michael Bazzell" "Accountant"
"Michael Bazzell" "software programming"
"Michael Bazzell" "International Police Association"

The quotation marks in the above searches are vital to the queries. They inform the search engine to only look for exactly what is presented. This will prevent Google and others from adjusting your search in order to "help" you. Each search engine that you use will likely give different results. You may want to try variations of your name. In my case, I would want to search "Mike" and "Michael". If you do not receive any results, you may want to repeat the search without the quotation marks.

Every engine has its own algorithm for search and also its own sneaky ways of collecting information during your search. Chapter Four will explain many ways to protect you while searching. For the purposes of this chapter, you only need to apply two policies.

First, never conduct these searches while you are logged into an email or social network account. If you are conducting queries on Google while logged into your Gmail account, Google stores this information about you. If you are searching on Bing while logged into your Facebook page, Bing now associates your queries with your profile. Overall, you do not want any companies to store your searches and associate them with you.

Second, you should not conduct these searches while using a web browser that knows a lot about you. All browsers store "cookies" that record the sites that you visit and the activity that you perform on the sites. Ideally, you should eliminate all of your cookies within a web browser before you conduct any searches. Chapter Four will explain further details. For now, this step is not vital for these basic searches.

Alternative Search Engines

There is no lack of search engines that could be used. While Google and Bing are the two main players, there are many other specialty engines that display results that the others miss. The following is a list of recommended engines for your pre-assessment.

Google	Google.com
Bing	Bing.com
Yandex	Yandex.com
Exalead	Exalead.com
Google Groups	Groups.google.com
Google News	News.google.com
Google Images	Google.com/images
Bing Images	Bing.com/images

Duck Duck Go (duckduckgo.com)

There are many people that do not trust Google due to their policies on data collection and advertisements. If you would like to conduct a query within a search engine that does not track you or record your actions, consider Duck Duck Go. This engine combines several sources to give you a collection of search results. None of your actions are recorded and the search engines that supply the content do not see your information. This can be a great search engine for daily queries. However, I believe that you will be missing many results if you do not use engines such as Google directly for the searches in this chapter. Chapter Four will outline additional steps that you can take in order to protect your privacy while on the internet.

Start Page (startpage.com)

If you want to take advantage of Google's search abilities but insist on hiding yourself from their intrusive monitoring techniques, you can use Start Page. Start Page searches Google for you. When you submit a search, Start Page submits the query to Google and returns the results to you. All Google sees is a large amount of searches coming from Start Page's servers. They cannot associate any traffic to you or track your searches. Start Page discards all personally identifiable information and does not use cookies. It immediately discards IP addresses and

does not keep a record of any searches performed.

All-In-One Search Tool (inteltechniques.com/osint/user.html)

I maintain a page on my website that will allow you to conduct a single query across multiple websites in one click. This is my preferred method when conducting a pre-assessment on someone. The website listed above will present many search fields that will allow you to execute a query on various services. The last search field at the bottom will allow you to execute any query on all of the listed services.

Figure 1.01 displays this page. Clicking the "Submit All" button will open a new tab for each service. This currently requires Firefox or Safari web browsers. Chrome and Internet Explorer may block the required code to perform this action. However, any browser can conduct individual queries through the listed services. This utility will search the following seventeen services.

Google
Google Results
Google Date
Bing
Yahoo
Yandex
Exalead
Google Groups
Google Blogs
Google FTP Search
Google Scholar
Google Patents
Google News
Baidu
Duck Duck Go
Qwant

Use the following box to document your progress. Knowing the date searched and whether you found a result or not might be useful later in the removal process. Placing a check mark next to each result can indicate that the data was

later removed. This same worksheet should be used at the end of your removal campaign to verify success.

Date:	Result:	Engine:	Description:
_____	_____	Google	Google Results
_____	_____	Google Date	Recent Results
_____	_____	Bing	Bing Results
_____	_____	Yahoo	Yahoo Results
_____	_____	Yandex	Russian Results
_____	_____	Exalead	Business Results
_____	_____	Google Groups	Newsgroups
_____	_____	Google Blogs	Blog Entries
_____	_____	Google FTP Search	FTP Documents
_____	_____	Google Scholar	Documents
_____	_____	Google Patents	Patents
_____	_____	Google News	Online News
_____	_____	Baidu	Chinese Search
_____	_____	Duck Duck Go	Anonymous Search
_____	_____	Qwant	Social Networks

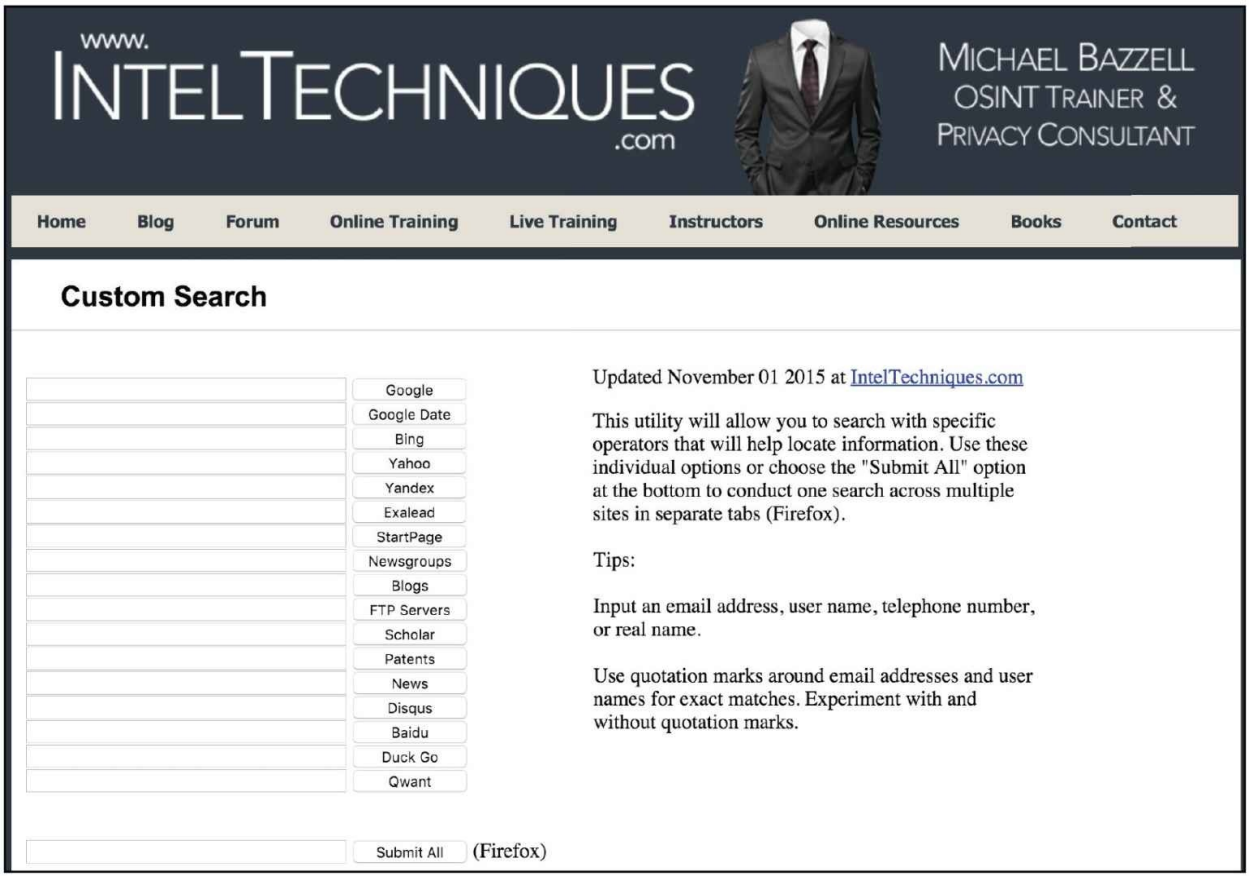


Figure 1.01: A custom search page on IntelTechniques.com.

Ancestry Records

Most readers will know someone in their life that collects information about the family's history. In previous decades, this meant writing relatives' names and lineage onto a piece of paper and distributing copies at the next family reunion. Today, this means uploading all of the data to a public website. These websites do not display social security numbers of the living, but the information can be quite intrusive. If you are listed in an online family tree, it is likely that the following information is available about you.

Full Name
Date of Birth
Parents' Names
Siblings' Names
Children's Names

City of Current Residence
City of Birth

With this information, a private investigator could quickly hone in on your actual address. He or she could obtain a copy of your birth certificate and would know your mother's maiden name. There are several financial institutions that still mistakenly rely on this piece of information for identity verification. Knowing your child's names could help answer security questions and jeopardize their safety if you are a targeted individual. I believe this type of personal information has no place on the internet. Identifying this exposure can be difficult. Visit the following websites and conduct a preliminary search on your name or your parents' names.

Date:	Result:	Service:	Website:
_____	_____	Ancestry	ancestry.com
_____	_____	Family Search	familysearch.org
_____	_____	Mocavo	mocavo.com
_____	_____	Roots Web	rootsweb.com
_____	_____	Geneanet	en.geneanet.org
_____	_____	My Heritage	myheritage.com
_____	_____	One Great Family	onegreatfamily.com
_____	_____	World Records	worldvitalrecords.com
_____	_____	My Trees	mytrees.com
_____	_____	Find My Past	findmypast.com

If you find information about you or your immediate family, document the results with a "Yes" or "No" in the results column and keep this in mind when data removal is discussed later. The majority of the content on these websites is user submitted and can include sensitive information. Fortunately, you will be able to remove most of the personal information that you locate.

Some of these services will require you to be a paid member in order to conduct a full search. I do not recommend purchasing a subscription for the sole purpose of looking for yourself. Instead, I encourage you to search these specific websites through a search engine with your details included. Consider the

following example. You want to search any ancestry.com services for your name and address. For this scenario, assume that your name is George Bluth and you reside in Alton, Illinois. Submit the following search to several search engines.

site:ancestry.com “George Bluth” “Alton”

This informs the search engine that you only want to search ancestry.com, but also that you want to search every indexed page at that domain. Your name within quotation marks mandates that your exact name is present on the page as well as the term Alton. This may display results that you cannot find manually by searching the actual website.

Email Addresses

After you have identified the various websites that display your residence and telephone information, you should identify services that are connected to your email address. In years past, providing an email address to a company or service did not seem too alarming. Today, this unique identifier can be used to create a detailed record about you and your interests. To obtain accurate results of your email search, quotation marks must be used before and after your email address.

Figure 1.02 displays a Google search result for one of my email addresses. The listed websites are present because my email address is associated with my website. Notice the blue “Sign in” button in the upper right corner. That is an indication that I am not logged into any Google account which provides a small layer of privacy. Chapter Four will discuss the three main levels of online privacy and how to apply the level that works best for you.

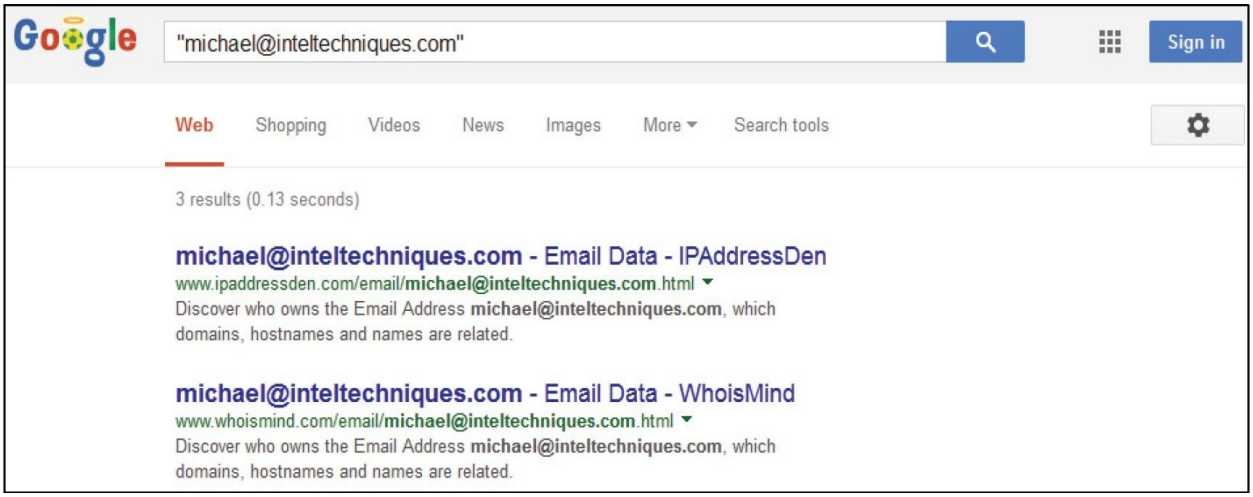


Figure 1.02: A Google search result from an email address within quotation marks.

It is important to know what information is associated with your email address. Many people will conduct a quick search on your address when you contact them. If you locate embarrassing or inappropriate content, you may want to use a different email account when corresponding about business or other important matters. The information found during this search will be very difficult to remove. You may consider switching to a new email address.

User Names

You may wish to search for any social networks that you have visible on the internet. You probably remember your Facebook and Twitter pages, but how many networks did you create and abandon when they lost popularity? We often forget about MySpace, Friendster, and other profiles that we no longer use. Often, those profiles are still visible and may contain personal information. Consider identifying any accounts that you wish to delete.

The easiest way to discover any accounts that may still be lingering is to search by your user name. Since we usually use the same user name for numerous accounts, you may look at known social networks for a hint. You may want to search your Twitter name, Facebook profile name, or the first part of your email account. If your email address is “michaelb911@yahoo.com”, you may want to search for only “michaelb911”. Locating your old network profiles can be a

daunting task. Fortunately, we have services to assist us.

KnowEm (knowem.com)

KnowEm (knowem.com) is one of the most comprehensive search websites for user names. The main page provides a single search field which will immediately check for the presence of the supplied user name on the most popular social network sites. In the main page, a user name search provides information about the availability of that user name on the top 25 networks. If the network name is slightly transparent and the word "available" is stricken, that means there is a subject with a profile on that website using the supplied user name. When the website is not transparent and the word "available" is orange and underlined, there is not a user profile on that site with the supplied user name. For your purposes, these "unavailable" indications suggest a visit to the site to locate your profile.

The “Check over 500 more” link in the lower left corner of the page will open a new page that will search over 500 social networks for the presence of the supplied user name. These searches are completed by category, and the "blogging" category is searched automatically. Scrolling down this page will present 14 additional categories with a button next to each category title stating "check this category". This search can take some time. If you had a unique user name that you liked to use, the search is well worth the time.

Location Based Searches

You have now likely located the publicly available content that we will attempt to remove from the internet. This will often be easy to find because it is searchable by your name, address, or telephone number. However, there is often social network information that is defined by the location from where it was posted. Many services such as Twitter and Instagram embed the GPS coordinates of the user along with the posted content. This can quickly identify where a person lives or works. It is likely that you are not uploading this type of detail. However, your children, friends, and family may not think about this type of technology and unintentionally compromise your privacy. You should consider conducting searches based on location as well as text. The easiest way to do this is through Echosec.

Echosec (app.echosec.net)

This simple website allows you to zoom to any location and query social network posts that were submitted from that location. Conduct the following steps to search your targeted area.

- ✓ Connect to app.echosec.net in your web browser.
- ✓ Either navigate through the interactive map or type your address directly into the search box in the lower left.
- ✓ Click the "Select Area" button in the center bottom portion of the page. Draw a box around the target area and release the mouse.
- ✓ Navigate through any results displayed below the map.

The square icons within the map identify Twitter and Flickr posts by the location they were uploaded. This type of sharing can quickly disclose your home address, your employer, or your relatives' addresses.

After searching your home, consider a query for your workplace, relatives, or child's friends' houses. You will likely locate personal information that would have been difficult to find based on keyword searches alone. This can be a useful technique to find a child's account when they are unwilling to share it with you. This will only search recent Twitter posts. You may also consider the following services which will allow you to search Twitter archives by location.

MapD: MIT (http://mapd.csail.mit.edu/tweetmap/)
MapD: Harvard (http://worldmap.harvard.edu/tweetmap)

Instagram

Echosec will no longer display Instagram results in the free version. While not as pretty or user friendly, I do have a solution for locating these posts by location. Navigate to the following website and enter the GPS coordinates of your desired

location on the last line.

http://inteltechniques.com/OSINT/instagram.html

Be sure to use either Chrome or Firefox as your web browser. Click the “GEO View” button in order to display any posts with geo-tagging enabled from your target location. Clicking on the Instagram hyperlink will open the post. If your result looks “garbled”, you are missing a browser plugin that allows you to display XML/JSON files. I recommend installing the plugin “JSON View” to your browser of choice.

If you need the GPS coordinates of a location, search the address within Google Maps, right click on the building, and select “What’s Here”. This will display the coordinates in the upper left corner of the map.

Now that you have identified the basic types of information that is publicly visible about you through search engines, consider the content that you would like removed. Most privacy seekers want to eliminate any reference to their home address and telephone number. Some people just want to remove those embarrassing photos posted in college. Regardless of your situation, the later chapters in this book will assist with erasing this data. This assessment was only a first step in establishing the scale of information available about you. It is recommended that you conduct the following self-background check to identify more details.

Chapter Two

Self-Background Check

At this point, you have completed the basic steps to identify your personal information visible in public view from search engines. You are now ready to conduct a complete self-background check. This will be done in two phases. The first phase will include only public internet websites that anyone could use to find you. The second phase will involve you requesting personal reports that will identify information stored about you in private databases not visible from the internet. The entire check should be completed at least once every five years.

Phase One: Public Websites

Later chapters outline the removal processes for the majority of the websites that display your personal information. Before attempting removal, you should identify those sites that have a record visible on you. Navigate to each of these websites and conduct a search on your name, address, telephone number, or user name as appropriate. Be sure to take note in the accompanying worksheet of which services possess information that you wish to remove.

People Directories

People directory website removal will be explained later. Before you can target these websites to remove your information, you should identify which services contain information about you. You should also consider searching for your children’s information. If personal information is located, conduct the removal process for that specific website.

Telephone and Address Directories

While these are not technically people directories, searching your home address or telephone number on these websites will likely display your name as an association. Some of these will not allow removal. However, a strategic disinformation campaign will often mask the results. Use the following table to thoroughly identify any compromised information. Attempt searches by name, address, and telephone number as appropriate for each site.

People Directories

Date:	Result:	Engine:	Website:
_____	_____	Spokeo	spokeo.com
_____	_____	Pipl	pipl.com
_____	_____	Yasni	yasni.com
_____	_____	ThatsThem	thatsthem.com
_____	_____	Zabasearch	zabasearch.com
_____	_____	Intelius	intelius.com
_____	_____	ZoomInfo	zoominfo.com
_____	_____	InfoSpace	infospace.com
_____	_____	PeepDB	peepdb.com
_____	_____	Radaris	radaris.com
_____	_____	WebMii	webmii.com
_____	_____	Genie	reversegenie.com
_____	_____	PeekYou	peekyou.com

Telephone Directories

Date:	Result:	Engine:	Website:
_____	_____	411.com	411.com
_____	_____	WhitePages	whitepages.com
_____	_____	YellowPages	yellowpages.com
_____	_____	Addresses	addresses.com
_____	_____	InfoSpace	infospace.com
_____	_____	SuperPages	superpages.com
_____	_____	411.org	411.org
_____	_____	SearchBug	searchbug.com
_____	_____	Genie	reversephonelookup.com
_____	_____	Detective	phonedetective.com
_____	_____	Reverse Genie	reversegenie.com
_____	_____	Phone Tracer	freephonetracer.com
_____	_____	Privacy Star	privacystar.com
_____	_____	TrueCaller	truecaller.com
_____	_____	PeekYou	peekyou.com
_____	_____	WhoCalld	whocalld.com
_____	_____	ThatsThem	thatsthem.com
_____	_____	NumberGuru	numberguru.com
_____	_____	MrNumber	mrnumber.com
_____	_____	10 Digits	10digits.us

Social Networks

If you use social networks, you should occasionally look through your profiles for any sensitive data that reveals personal information. Even if you no longer use social networks or deleted your account completely, you cannot ignore these sites. Your family and friends are still likely to post sensitive information about you. It could be a photo identifying your home address, vehicle license plate, or the location of your child's favorite hangout. It could also be a family member posting your telephone number to other family members, intending to be helpful. Searching the publicly available information on these sites is easy. The websites listed here will display a search option to find the most common information. Some services require you to be logged into an account in order to search their data. If you do not already have an account on a service, I do not recommend creating one for this purpose.

Date:	Result:	Network	Website:
_____	_____	Facebook	facebook.com
_____	_____	Twitter	twitter.com
_____	_____	LinkedIn	linkedin.com
_____	_____	Google+	plus.google.com
_____	_____	Tumblr	tumblr.com

Facebook

The Facebook data visible about you may extend beyond the content that is visible on your main profile page. There is often additional personal information leaking into other areas of the network. Use the following techniques to locate further details about your own profile and those of your family. This may help you decide if deleting your entire account is the way to go.

Facebook collects a lot of additional information from everyone's activity on the social network. Every time someone "Likes" something or is tagged in a photo,

Facebook stores that information. Until recently, this was very difficult to locate, if not impossible. You will not find it on the target's profile page, but the new Facebook Graph search allows us to dig into this information.

In order to conduct the following detailed searches, you must know the user number of your account. This number is a unique identifier that will allow you to search otherwise hidden information from Facebook. The easiest way to identify the user number of any

Facebook user is through the IntelTechniques website. While you are on your main profile, look at the address (URL) of the page. It should look something like Figure 2.01.

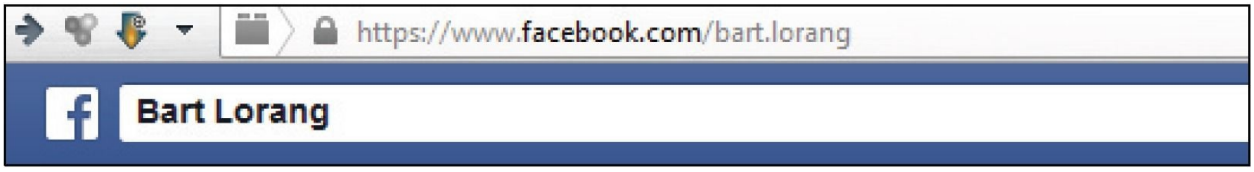


Figure 2.01: A web address (URL) of a Facebook Profile.

The full address of the page is https://www.facebook.com/bart.lorang. This identifies "bart.lorang" as the user name of the user. In order to obtain the user number, place this user name into a Facebook Custom Search tool located in the resources section of the Intel Techniques website at **inteltechniques.com/OSINT/facebook.html.** Figure 2.02 displays this search tool that translated this user name into a user number.



Figure 2.02: A Facebook user number.

The number that you see in this result is the person's user number on Facebook. This data will allow us to obtain many more details about the account. Repeat this process on your own Facebook page. If I want to see any photos on Facebook that you have "liked", I can type the following address into a web

browser. Replace 651620441 with your own Facebook user number as in the example that can be seen at the profile address of https://www.facebook.com/search/651620441/photos-liked. This basic structure contains the website (facebook.com), the action (search), the user number (651620441), and the requested information (photos-liked).

Since these are photos that were "liked" by you, the results will include photos on other people's pages that would have been difficult to locate otherwise. If I had asked Facebook for this information with only your name, I would have been denied. If I asked within the search filter options mentioned earlier, I could only search by general name and could not identify a specific user. If you have a common name, this would not work. The method described here works because I know your user number. There are many other options with this search. I can navigate to the following addresses to see more information about you (user number 651620441). Explanations of each address will be explained after.

https://www.facebook.com/search/651620441/places-visited
https://www.facebook.com/search/651620441/places-liked
https://www.facebook.com/search/651620441/pages-liked
https://www.facebook.com/search/651620441/photos-by
https://www.facebook.com/search/651620441/photos-liked
https://www.facebook.com/search/651620441/photos-of
https://www.facebook.com/search/651620441/photos-commented
https://www.facebook.com/search/651620441/videos
https://www.facebook.com/search/651620441/videos-by
https://www.facebook.com/search/651620441/videos-of
https://www.facebook.com/search/651620441/videos-liked
https://www.facebook.com/search/651620441/videos-commented
https://www.facebook.com/search/651620441/apps-used
https://www.facebook.com/search/651620441/friends
https://www.facebook.com/search/651620441/events
https://www.facebook.com/search/651620441/events-joined
https://www.facebook.com/search/651620441/stories-by
https://www.facebook.com/search/651620441/stories-commented
https://www.facebook.com/search/651620441/stories-tagged
https://www.facebook.com/search/651620441/groups
https://www.facebook.com/search/651620441/relatives

The “places-visited” option will display locations that your profile states you have physically visited and allowed Facebook to collect the location information. This is often completed through a smart phone, sometimes unintentionally. This can be used to disprove alibis or verify trips.

The “places-liked” option will display any physical locations for which you have clicked “like”. This will often identify vacation spots, favorite bars, and special restaurants. This can be priceless information for an investigator or skip-tracer.

The “pages-liked” option will display any Facebook pages that you visited and clicked “like”. This will often display your interests such as a favorite sports team, musical group, or television show. These results will include a button labeled “liked by”. Clicking this will identify everyone on Facebook that liked that item. This can quickly identify the people that visit the same hole-in-the-wall bar that you frequent.

The “photos-by” option will display Facebook photos that were uploaded by you. These will likely already be visible on your photos page. However, this search could potentially reveal additional images.

The “photos-liked” option was explained on the previous page. This can be beneficial by showing photos that you have liked, most of which you have probably long forgotten. If the photos of interest are on someone else’s profile that is not private, you will be able to see all of them.

The “photos-of” option will display any photos that you have been tagged in. This search has already proven very effective in many investigations. This will immediately locate additional photos of you that are not available on your profile. This is helpful when the photos are private on one person’s page, but not others.

The “photos-commented” option will display any photos on profiles where you left a comment on the photo. This can be important because you may not have “liked” the photo or been tagged in it. The option may produce redundant results.

The “videos” option will display videos visible on your profile. These may or may not be directly connected to the target. They could also be videos linked to the original source with no personal ties to the subject.

The “videos-by” option will display videos that were actually uploaded by the target. These will be much more personal to the subject and will usually include more relevant content.

The “videos-of” option is similar to the “photos-of” filter. This will display videos that supposedly contain images of the target within the video itself. It could be compared to “tagging” someone inside a video.

The “videos-liked” option will display any videos that the target clicked “like”. This can also be used to establish personal interests of the target and are often of interest to parents.

The “videos-commented” option will display any videos on profiles where the target left a comment on the video. Again, this can be important because the target may not have “liked” the video or been tagged in it. The option may produce redundant results, but it should always be checked.

The “apps-used” option will display the apps installed through Facebook. These are usually games that can be played with other people. Many of these specify the environment that they work with such as “IOS”. This would indicate that the target is using an iPhone or iPad instead of an Android device.

The “friends” option should display a list of all of the target’s friends on Facebook. This will be the same list visible on the main profile page. If you receive no results, the target likely has the friend’s list set to “private”.

The “events” option will display any Facebook events that your target was invited to attend. These often include parties, company events, concerts, and other social gatherings. This will usually display events that are not listed on the target’s profile.

The “events-joined” option will only display the Facebook events at which you acknowledged attendance. This could be in the form of a “R.S.V.P.” or confirmation by the target that they are currently at the event. This has been used to question the alibies of suspects.

The “stories-by” option will display any public posts you have made. This can often identify posts that are not currently visible on your profile.

The “stories-commented” option will display any public posts by any users on which you entered a comment. This could be useful in identifying communication between you and a private profile. The standard privacy options do not prevent a search of your comment history on public posts.

The “stories-tagged” option will display any posts that you tagged. This tagging is usually performed because of an interest in the post.

The “groups” option will display any groups that you are a member of. This is beneficial in identifying your stronger interests. In my experience, an individual must only have faint interest to “like” something. However, the interest is usually strong if a group related to the topic is joined.

The “relatives” option will display a list of people that you have identified as a relative. Often, this will display relatives even if you have your friends list set to “private”.

Custom Facebook Search Tool

You may now be wondering how you are going to implement all of these searches in an easy format. Navigate to the following website in order to access an all-in-one option.

http://inteltechniques.com/osint/facebook.html

This page will allow you to conduct all of the Facebook Graph searches that were mentioned in this chapter. Copy and paste your user name from the profile address into the second option to identify your user number.

The next group of searches will display the “liked”, “tagged”, and “by” information that I previously discussed. Make sure you are logged into a Facebook account for this to function. I also recommend using the Firefox browser. Chrome occasionally blocks the script required to make this work.

Phase Two: Private Databases Reports

The websites and services in this section can be queried at any time. Most of these businesses do not publicly share your information and do not offer opt-out methods. The data stored is shared with other businesses and can affect your credit score, insurance rates, and ability to obtain a line of credit. While you cannot remove your profile from these databases, you can correct any errors in the reports. These corrections could save you money if you find yourself paying rates that appear to be higher than normal.

Free Credit Report (annualcreditreport.com)

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 a free credit report. The only official government supported free credit report website is at annualcreditreport.com. This website allows you to view your credit report without any fee once yearly from each of the three credit bureaus. This means that you actually 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:

- ✓ In January, connect to annualcreditreport.com and request an Equifax report.
- ✓ In May, request a free report from Experian.

- ✓ In September, request a free report from TransUnion.

These months can be adjusted. The important element is that you are viewing your credit report throughout the year. The process for viewing your report varies by state. The website will explain every step. When you receive your report, pay close attention to the entire document. Further, I believe that the following sections deserve extra scrutiny.

- ✓ The inquiries section of a credit report will identify any companies requesting a copy of your report. This will usually be creditors verifying your details for a loan request.

- ✓ The non-impact section of a credit report includes requests from employers, companies making promotional offers, and your own query requests.

- ✓ The address information of a credit report will identify any addresses used for current and previous lines of credit. If you see an unfamiliar address, report this.

- ✓ The open accounts section of a credit report will identify any unused open accounts and a contact number to close the account if desired.

- ✓ The closed accounts section will verify that an account was closed.

LexisNexis (lexisnexis.com)

A later chapter will explain how to conduct an advanced removal from LexisNexis. This includes instructions to opt-out of non-public databases. Whether or not you apply these techniques, you should request your personal file from this company. Even if you requested information removal, you will find that the company maintains a file on you. This does not mean that your information is available to the public. The steps below will allow you to review the data LexisNexis stores about you.

- ✓ Navigate to personalreports.lexisnexis.com/pdfs/CD107_CP-File-Disclosure-Request-Form_pg-3.pdf and print the form.

- ✓ Navigate to lexisnexis.com/privacy/for-consumers/CD307_Accurint_Person_Report_Info_Form.pdf and print the form.

- ✓ Print a redacted copy of your driver's license as discussed in Chapter Three. Mail it and both forms to the address listed in the upper right corner of each form.

Westlaw / Clear / Thompson Reuters (clear.thomsonreuters.com)

This is another large company that was discussed earlier. The detailed content of your personal report will probably surprise you. This report can often identify attempted fraud or identity theft conducted in your name. Follow these instructions to obtain your free report:

- ✓ Navigate to static.legalsolutions.thomsonreuters.com/static/pdf/info_request_form and print the form.

- ✓ Complete the document with your real information. The information is only used to verify you for the report. New information is not added to any databases. Print a copy of your redacted driver's license (Chapter Three). Mail it and the printed form to the address listed.

Acxiom (acxiom.com)

Acxiom offers two types of personal reports. The first is a fraud detection and prevention report. This report exists if you have returned a large amount of merchandise to retail stores. It is used to identify fraud and probably does not apply to the audience of this book. Unfortunately, this report costs $5.00 to obtain and can be found at isapps.acxiom.com/rir/rir.aspx.

The second option is the background screening report. This is provided to potential employers that request the product. Inaccurate information in this report could explain difficulty in obtaining employment. This report is free.

- ✓ Telephone 800-853-3228 and select option 3. State the following to the customer services representative.

- ✓ "I believe that there are errors on my background screening report. Per the rules of the Fair Credit Reporting Act, I would like to request a free copy of my report."

Sterling Infosystems (sterlinginfosystems.com)

This is another service that provides employment related consumer reports to potential employers. An online or mail request can be conducted.

- ✓ Navigate to sterlingbackcheck.com/About/Fact-Act-Disclosure.aspx and then complete the online form. Provide a valid email address to receive your digital report.

Innovis (innovis.com)

This is another consumer credit information company that is similar to Equifax, Experian, and TransUnion. One big difference is that you cannot obtain your Innovis credit report through the free website annualcreditreport.com. Innovis encourages mailed requests for a personal credit report, but the automated telephone system is easier and more efficient.

- ✓ Telephone 800-540-2505 and listen to the recorded message. Choose "1" for the first two menu options. You will then be asked to enter your social security number, date of birth, zip code, and numeric portion of your home address to verify your identity.

- ✓ You will be informed that you can obtain a free credit report if you are unemployed, on public assistance, or suspect that you may be the

victim of identity theft. The first two choices are obvious, but the third is open to interpretation. If you believe it is POSSIBLE that you are a victim of identity theft and want to verify this through a credit report, select option "4" as instructed.

Approximately one month before I requested credit reports from Equifax, Experian, TransUnion, and Innovis, I contacted my bank and changed my telephone number to an anonymous forwarding number. The only credit report that obtained this new number was Innovis. The number is now associated with my name and will be shared with several companies. This intentional form of disinformation will help mask my real telephone number from the public.

Core Logic (corelogic.com)

Core Logic is a consumer information powerhouse. If you complete the opt-out process described later, the company will no longer share your information. However, they still maintain your profile and will allow you access to the report.

- ✓ Use your personal anonymous email account explained previously and create an email message with the subject of "Opt-Out" to srumph@corelogic.com. State the following and include your name, home address, and date of birth.

- ✓ "Per your policy as published at corelogic.com/privacy.aspx, I would like to request my consumer report maintained by Core Logic."

CoreLogic Credco is one of the largest credit-related credit reporting agencies and is often used by mortgage lenders. Your consumer file can contain previous homeownership and mortgage information, rental payment history, any reported delinquencies, and other debt obligations such as child support. You are entitled to a free copy once every 12 months.

- ✓ Print a written letter stating "I would like a disclosure copy of your consumer file in my name". Include your full name, social security number, current and previous addresses, and date of birth. You will need to send a copy of one of the following.

Valid driver's license
Social Security card
State identification
Military identification

- ✓ You will also need to send one secondary form of identification which can be any of the following.

Valid driver's license
Utility bill with your current address
Rental lease agreement
Mortgage statement
Bank statement
State identification

- ✓ Send everything to the following address.

CoreLogic Credco, LLC
PO Box 509124
San Diego, CA 92150

SageStream

SageStream, LLC, formerly known as IDA Inc., is a credit reporting agency that produces credit reports and scores from their repository of consumer information contributed by a wide array of companies. If you believe that information contained in your report is not accurate, you can take steps to dispute it. To obtain your free personal consumer report, you will need to submit a signed, written request to SageStream with the information listed below. For security purposes, they must verify your identity by receiving a minimum of two copies of verification documents that match the information you provide with the request.

- ✓ Create a written request with signature that includes your full name, home address on file, anonymous phone number, social security number, and date of birth. Include copies of at least two of the

verification documents listed below that substantiate the personal information that you provided.

Driver's license or Government ID
Recent utility or phone statement, produced 60 days ago or less
Social Security card
Birth certificate
U.S. passport picture page

- ✓ Mail your request to the following address.

SageStream, LLC Consumer Office
PO. Box 503793
San Diego, CA 92150

Safe Rent (corelogic.com)

If you currently rent your residence or plan to seek rental housing in the future, you should request a copy of your consumer file maintained by Safe Rent, a Core Logic company. You must complete a form and submit via fax or postal mail.

- ✓ Print the form located at the website corelogic.com/downloadable-docs/nbd03-104-disclosure-request-web-packet.pdf.

- ✓ Complete the form with your real information and submit via postal mail to the address on the document.

- ✓ There is a fee to access a report. However, there are certain situations that allow for a free report. If you meet ANY of the following conditions, the fee will be waived:

Denial of your housing application
Required to have a deposit not required by others
Required to have a cosigner

Assessed a higher rental rate than others
Denied employment or promotion
Reassigned or terminated
Unemployed or filing for unemployment within 60 days
Public welfare recipient
Have reason to believe your file may contain errors

I believe that practically everyone can qualify through one of these conditions. The last option can apply to anyone that believes “typos” are possible on their report. Follow the instructions on the form and expect your report within two weeks.

Insurance Services Office (iso.com)

Your vehicle and home insurance rates can be influenced by your loss history report. Inaccuracies in this report can cause unnecessary rate increases. The Insurance Services Office will provide a free copy of your report. Included in this copy are any losses reported to your insurance company in the past five years.

- ✓ Place a telephone call to 800-627-3487. Provide the information requested for verification purposes. Your report will arrive via postal mail in about one week.

Tenant Data (tenantdata.com)

This is another rental data agency that reports resident history and a tenant profile of rental prospects. If you do not rent a home, this would not apply to you. If you would like to see the data collected about you and your rental history, complete the following.

- ✓ Navigate to the following website and print, complete, and send the form: tenantdata.com/downloads/AuthorizationforFileDisclos_new.pdf

Experian Rent Bureau (experian.com)

Experian maintains their own database of rental history and creates profiles of renters.

- ✓ Navigate to experian.com/assets/rentbureau/brochures/request_form.pdf and print, complete, and send the form.

Chex Systems (consumerdebit.com)

If you have been the victim of identity theft or any type of financial fraud, criminals may be attempting to write checks against your accounts. Many automated systems will stop this fraudulent activity, but may not notify you of the issues. You can request a report of any negative impact on your checking accounts from two sources.

- ✓ Navigate to the website consumerdebit.com/consumerinfo/us/en/chexsystems/report/index.htn Click “Agree” to begin the online form submission. Complete all required fields and click “Submit”. You should receive your report via postal mail within five days.

TeleCheck (firstdata.com)

The second company to request a checking report is TeleCheck. The request process is more demanding than the previous report, and the submission must be sent via postal mail.

- ✓ Open a copy of your custom opt-out form created in Chapter Three. Include your anonymous telephone number and your social security number. All other information can be removed from the document except the copy of your driver’s license. Print the form when completed.

- ✓ Package the previous form, a copy of any utility bill or tax statement, and a voided check. Send the documents to the following address.

TeleCheck Services, Inc.
Attention: Consumer Resolutions-FA
PO Box 4514
Houston, TX 77210-4514

Retail Equation (theretailequation.com)

When you return a product to a retail or online store, your information is recorded and shared with several companies. This includes the location, product, amount, and reason for return of the product. This database was created to combat exchange fraud, and you are likely in it. If you are curious about the information being shared about your shopping habits, you can request a copy of your report.

- ✓ Create an email addressed to returnactivityreport@theretailequation.com. Include your name and anonymous telephone number in the message.

- ✓ You will be contacted by the company to process your request. If you are asked for a transaction number, state that you do not have that information.

Medical Information Bureau (mib.com)

When you apply for medical insurance, the provider will seek your report from the Medical Information Bureau. This report will include information such as height and weight, and identify any noteworthy gains and losses. Depending on your medical history, the additional information will vary. This report can influence the amount of money that you pay for medical insurance. Verifying the accuracy of this report is important when seeking new coverage.

- ✓ Navigate to

www.mib.com/disclosuretransfer/disclosureservice/formrequest and complete the online request form. Select “For Yourself” on the first screen and click “next”. Provide only the following information. The additional fields are optional.

Name
Gender
Mailing Address (PO Box)
Anonymous Telephone Number
Birth Date
Social Security Number

- ✓ Confirm the information and expect a report within two weeks.

Milliman IntelliScript (rxhistories.com)

This company stores information about your prescription drug history. These reports are shared with insurance companies that determine your insurance rates. If you are seeking new insurance quotes, inaccuracies in this report can be devastating. You may obtain a free copy of your report.

- ✓ Telephone 877-211-4816. Be prepared to disclose your name, mailing address, telephone number, date of birth, and last four digits of your social security number. Expect a mailed report within ten days.

National Consumer Telecom and Utilities Exchange (nctue.com)

This database is managed by Equifax. It provides fraudulent activity and delinquencies involving utilities and related services. These reports are obtained by companies before utilities are authorized for a building. If someone has fraudulently used your personal information, this report will disclose the details.

- ✓ Telephone 866-349-5185 to speak with a representative. State that you want to request a free copy of your “data report”. Be prepared to disclose your social security number, name, and date of birth. While I

usually never recommend providing this information, it is only used to verify your identity to the company. If you have ever had any utilities in your name, they already have this information. Supplying the details does not put you at additional risk.

- ✓ You will be placed on hold while your report is retrieved. After the report is generated, you will receive a confirmation number. The actual report will arrive within three business days.

- ✓ Visit www.nctue.com/Consumers and complete the Opt-Out request.

Social Security Administration (ssa.gov)

Beginning in 2012, the social security administration no longer sends reports via postal mail. This cost savings measure requires you to view your statements online. If you plan to conduct a credit freeze, be sure to complete this process first. The account creation on this website cannot be completed with a credit freeze in place.

- ✓ Navigate to ssa.gov/myaccount and click the button labeled "Sign in or Create an Account". Click the "Create an Account" button and provide the requested information. Choose a secure password and view this statement yearly. If anyone attempts to use your social security number for payments, this statement will disclose the fraud.

The reports in this phase of the chapter are optional and none of them will help you hide from the internet. Many will not apply to you. Only you can determine which companies are likely to possess information about you. If you find yourself continuously trying to figure out why you tend to pay more for various services than other people, your answer may be in one of these reports. Generally, requesting a copy of your own consumer report does not adversely affect your credit score since it is not considered to be a "hard" inquiry that a potential creditor would make when you apply for credit or open an account.

Chapter Three

Preparation

Before you attempt to remove any of your personal information from the internet, you must take several steps to prepare yourself for this journey. While most of this book can be read in any order, this chapter should be read in its entirety before proceeding. Failure to have these preparations in place will cause some of the methods described in this book to take longer than necessary. Even worse, it will make some of the methods ineffective. Before you prepare to start removing your personal information from the internet, you should evaluate how your information became accessible to the public.

Rule # 1: Stop Giving Out Your Information!

The first obvious thing to discuss is how you provide your personal information to the world. Every month, you provide many personal details about you and your family that get sold to numerous companies. Large databases are created that include a profile on you that is passed around and updated continuously. The following are three examples of the information that you provide unknowingly.

Reward Cards & Loyalty Programs

As a frugal person, I love these money saving cards. As a privacy advocate, I hate them. Many grocery stores, cafes, restaurants, and discount clubs offer them to save you hundreds of dollars every year. When you use these cards, everything you buy is associated with your name and address. When companies contact the rewards card provider looking for new customers, your information often gets sold if you fit a certain criterion.

For example, a shoe company wants to know all of the customers of a specific grocery store that purchased magazines associated with running or fitness. That grocery store can easily conduct a search and create a list of reward program customers that fit the criteria and sell that list to the shoe company. This list could include your name, home address, telephone number, email address, and shopping habits. Now, you may get bombarded with unwanted advertisements in the mail, spam in your email inbox, and telephone calls offering fitness themed vacations. This same information may then get passed on to another company. In one extreme scenario, The New York Times reported in February of 2012 that the department store Target began sending advertising for expectant mothers to a female high school student in Minneapolis. The package included coupons for baby items addressed to the minor. The father was furious and complained to the store. He accused Target of encouraging minors to become pregnant. He later was informed by the minor that she was indeed pregnant. This automated package was sent to her after analyzing other shopping habits of the minor.

I am not against the continued use of the loyalty cards and programs, but users should change the way that they apply for the program. The first step is to simply stop providing accurate information. Very few of these programs verify the information provided. If you sign up for one of these programs, change the spelling of your first and last name. If your last name is Laporte, use Lepurt. It is enough to confuse the system but still be accepted by you. More importantly, never provide your home address and telephone number. This chapter will discuss what to use as an address and phone number if you want to receive information from the company.

Many people use a completely false name. For programs that rely on the use of a physical card, such as a grocery store, there is little harm in providing a false name. The only purpose of the card is to save the money immediately at checkout. Be aware, however, that the debit or credit card you use will be associated with that loyalty card. Cash is king. For those programs that demand to see your identification before issuing a card, use your real name and tell them you recently changed your address.

Utility Bills

When you have your utility bills mailed to your residence, you are announcing to

the world where you live. Your utility company will obviously know your address, as they are providing a service to the structure such as electricity or water. They maintain a database of the utility bills sent to the customer including home address and phone number. This is often passed around to other companies that may have an interest in providing other services, and you will be targeted with advertising. These details are also made available to data mining companies that can be searched online. If you have a utility bill in your name mailed to your home address, internet searches will eventually announce the location where you and your family sleep at night.

Credit Cards and Financial Accounts

In 2011, I conducted an experiment. I called my credit card provider and requested an additional card in another name completely different from mine. A new card arrived promptly with the alternative new name, and my original account number. I began using this card for purchases, which were charged to my account. In three days, I conducted a detailed online search for my address that I use for the bill, and the fictitious name I had provided was now associated with my address. I was astonished. More details on how to use this technique to your advantage are discussed later.

While I will expand on ways to effectively use this technique, I urge you to only request a secondary card in an alias name after you changed the billing address to a PO Box. This will prevent the alias name from being directly associated with your home address. We must never be naïve and assume that this technique gives us complete anonymity. The credit card company will still know that you made the purchase. My point is that anyone can track you on the internet through your credit. The following methods will not replace the privacy of cash, but will eliminate much of the information available to the general public. This chapter is important for other concerns besides privacy. These methods will offer a new layer of security to protect you from identity theft and fraud. The advantage, as you will see in the following examples, is that the company of purchase will not know your real name.

Removal vs. Disinformation

Most of this book will focus on the techniques to permanently remove your

information from internet searches and data-mining companies. There will be moments that will require you to provide information to companies in order to add or remove their products or services. Sometimes you will need to provide details about you that will be verified by the company. This may include utilities that insist on a working telephone number for you and your date of birth with social security number. It could also be a website that requires your mailing address, email address, and mother's maiden name before granting you access to the website. Both of these situations can be handled in two extremely different ways.

You could take the standard approach that most people take and supply all of your real information and allow those details to be passed on to dozens of companies that will pass it on to dozens more. Alternatively, you can use a combination of anonymous information and disinformation. In this chapter, you will learn how to create an anonymous email address and telephone number that can be provided to companies without jeopardizing your privacy. As for the other information requested, I prefer to use disinformation. Disinformation is basically falsifying or manipulating the data in order to cause so much inaccurate information that it becomes difficult for companies to know the real details. Chapter Twelve will identify many ways to fool every data mining company in existence with disinformation.

Any time that someone requests your home and work address, you should evaluate whether that information is really needed for that scenario. If you are turning on water services at a building, that seems like a legitimate reason to disclose the address. You should not disclose your work address though, as it is not needed for that situation. If you are completing a membership form to join an association of bird watching enthusiasts, a post office box would be more appropriate. If you are making a purchase at a store that wants your address to add to the purchase history, you should be prepared to provide disinformation. One approach is telling them that you do not want to provide that information. This is usually met with hostility, and on rare occasion, refusal to sell the item or service. Instead, consider having a fake address ready to provide from memory. This should be an address that does not exist since you should not cause someone else to receive unwanted advertisements and mailings. Eventually, databases will start to associate you with this fake address, which is better than having no record in the database. Many companies will want your date of birth and social security number for their records. Unless you are requesting some

form of credit from the business, there is no need for them to have these details. Again, simply refusing often results in a difficult situation. Instead, consider providing a different date of birth. If it is something you will need to remember, reverse the month and day of birth and add 10 to the year. If your date of birth is 5/9/1970, provide 9/5/1980. Most people will avoid questioning your age, especially if you look older. The social security number is a little stricter. Usually, the company does not have anything in place to verify if the number is valid or assigned. Using someone else's number can be a crime. Instead, use one of the ten numbers reserved by the government to be used in advertisements. None of these special numbers will ever be assigned to a human and they do not look false as does 000-11-2222. Here is the complete list.

987-65-4320
987-65-4321
987-65-4322
987-65-4323
987-65-4324
987-65-4325
987-65-4326
987-65-4327
987-65-4328
987-65-4329

One scenario that provides a unique situation is when applying for employment. I do not recommend providing any disinformation on the application. Instead, use a post office box, the anonymous email address you will learn about here, and your real date of birth. The risk of this data being entered into a public database is minimal. Providing your social security number will probably be safe, but you could also fill in this space with "Upon hiring".

Whenever a company wants your personal details, stop and consider where this information may be copied or sold. In order for the rest of the techniques in this book to work, you must change the way that you provide your personal information. You could take every step in the book and eliminate everything out there, but signing up for a great credit card offer or filling out a form to win a new car with all of your information will reintroduce the details to the web based companies. You must change your habits.

Providing disinformation is not identity theft. Providing these small “errors” is not the same as creating a new account under another person’s name. The disinformation that you provide will only be enough to meet the collection requirements while masking your true information. It should never cause any fraud or financial gain to you.

Anonymous Email Address

Many of the websites that will be discussed throughout this book will require an email address to remove information. The email address provided to them will be stored by the company that it is submitted to and possibly sold to other businesses. If you use your real personal or business email address, this is counter-productive to the idea of eliminating personal information online. Therefore, you should never provide your current personal email address to any online website from which you want your information removed. To get around this, you will create two anonymous email addresses.

Gmail (gmail.com)

First, you should create a new account with a free email provider. Personally, I have many Gmail accounts from Google. Most privacy advocates hate Gmail and refuse to use their services. I agree that Gmail is invasive and scans all of your email for advertisement delivery. They are very open about that. However, I will not be using them for my personal email. For the purposes of this book, I will only use Google services as part of my effort to remove personal information and provide disinformation. I will not be using it for personal messages or “real life” content. Therefore, I recommend Google services for the methods discussed in this book. The services are reliable and free. After you have completed the removal process, you never have to use their service again if desired. Alternatively, you could choose any other email provider.

Navigate to gmail.com and click on “Create an Account” in the upper right corner. Provide any name that you want and create a password. For the gender and date of birth, you can also provide any data that you want, including false information. This will not be verified by Google. Gmail will ask you to pick an email address. I recommend choosing something with your real name in it. This address will be used to request removal of your personal information from select

companies that demand an email response. If your real name is Mike Smith, but your email address is BillJohnson@gmail.com, this looks suspicious. It may delay your request for removal. This email address should only be used during the removal methods described in this book. It should never be used for any other personal or business communication. The book will refer to this account as your new personal email address.

Many services that allow for information removal from their systems do not require you to email them. Instead, they will ask for your email address and will send an email directly to you. For these situations, you should use a completely anonymous forwarding email address that cannot be associated with you. You could create temporary forwarding accounts online, but after a short period of time, the email account is automatically terminated. My preference is to forward email from a permanent anonymous account to a personal account. This is different than the many providers that will give you a temporary account that works for a limited time. The next technique will give you a permanent email address that will always forward to any real email address of your choice.

Not Sharing My Info (notsharingmy.info)

This is an anonymous email forwarding service. Not only does it provide instant email delivery and a superb privacy layer, it is also free. Obtaining a permanent email address is immediate.

Navigate to notsharingmy.info and type in your actual personal email address. This can either be the new Gmail account that you created earlier, or a personal account that you check frequently. This may be the free Gmail, Yahoo, or Hotmail account that you use for your everyday email. I do not recommend using your business account since you probably have very little control over the account and access. When you click on “Get an obscure email”, the site will give you your permanent forwarding email address. My new email address is dhd9j@notsharingmy.info.

From now on, any time a person, automated service, or verification procedure sends an email to dhd9j@notsharingmy.info, the email will be forwarded to my new alias address of test@computercrimeinfo.com. This is all done behind the scenes and the original sender of the message will have no idea of what my real

email address is. However, if you respond to an email received from this account, the email will be sent from your actual personal account, not the anonymous account. This method should only be used for receiving emails.

For people I correspond with, I do not use this type of address. I save this type of address for use with verification techniques during information removal. Many websites that require a profile on the site also require a valid email address. As an example, when you sign up for Facebook, you must provide a valid email address. Once you do, Facebook will send an email to that address which you must read and click on a link within the email. Clicking on this link verifies to Facebook that they have an email address that belongs to you. By using the anonymous method described here, Facebook would only know your anonymous address, and not your real personal address. This also allows you to continue to receive messages from them without disclosing your personal account. Facebook occasionally restricts new accounts from Not Sharing My Info addresses, but the next service that will be discussed is always allowed.

The email address that is created for you from this service is rather generic and may be hard to remember. If you want a more custom email address, such as MikeBazzell@notsharingmy.info, you can do that as well. This will require you to sign into your Facebook account and convince a friend to sign up for the free service. I do not recommend this for two reasons. First, attaching this service to your Facebook page eliminates a layer of privacy that this service provides. Also, picking a custom address, such as your name, helps attach you to your anonymous account. For the purposes of this book, both are a bad idea. I recommend accepting the default address created for you. It is wise to write down the address immediately for future use. If you do decide to create a custom address, the instructions are on the same page as your new address.

According to the notsharingmy.info website, once an email message is delivered to the recipient, the message is not stored on their servers. This means that if you are using a service such as Gmail, Yahoo, or Hotmail, this company only has the content of your message for a short period of time. The site states that they do collect your IP address when you create your account, but that it is not associated with the email address or kept permanently. It should be noted that the service will always know your real email address, there is no way around that. The only way that this would be disclosed is through a legal request such as a subpoena or

search warrant. For the scope of this book, the only concern is keeping this information away from the general public. For the remainder of this book, any technique that mentions providing an email address should be given your new anonymous address created on this site.

Over the past few years, readers have advised the Not Sharing My Info would occasionally not work reliably. They reported outages for short periods of time. For a brief period, they were not accepting new accounts. At the time of this writing, the service appeared stable. However, if you would like more reliable experience with many additional features, I have a superior service to consider.

33 Mail (33mail.com)

While Not Sharing My Info is a great option, my favorite email forwarding service is 33 Mail. Similar to Not Sharing My Info, it will transfer any incoming email from your anonymous account to your real personal email address without the sender knowing. However, this service provides three additional features that make it superior to other email forwarding companies. It provides unlimited forwarding email addresses within one account, the option to reply from these addresses, and the ability to disable a forwarding address if desired. The following steps will explain how to create your new account and use the free service.

- ✓ Navigate to 33mail.com and create a new account at the "Get Started!" button.

- ✓ Provide your personal email address, choose a user name, and provide a password when prompted. Your user name should not have any association with you. It will be visible on all of your new forwarding email addresses. Somehow, I was able to obtain "NSA" as my user name.

- ✓ Choose the "Free" service plan when prompted. This is not selected by default.

- ✓ Check your personal email account and confirm the email from 33

Mail to verify your personal email address.

- ✓ You now have a new domain that you can use for any email address. Any email sent to that domain will be forwarded to your real email address. If an email was sent from anyone to removal@nsa.33mail.com, it would forward to my real email address.

- ✓ The next time you visit a website that asks for your email address; do not give it to them. Instead, make one up especially for them. For example, if the website spokeo.com demanded an email address for removal of my content, I might give them spokeo@nsa.33mail.com. Obviously, replace my domain listed here with yours.

You do not need to create any alias addresses on the 33 Mail website. This will happen automatically when incoming mail is received at their server. In order to demonstrate the service, I sent an email message to the following three accounts.

test@nsa.33mail.com
spam@nsa.33mail.com
removal@nsa.33mail.com

I immediately received the three messages in the inbox of my personal email address. Additionally, 33 Mail created the three aliases of Test, Spam, and Removal. If I were to start receiving a lot of unwanted email addressed to spam@nsa.33mail.com, I could click the “block” link next to that account, and that address would no longer be forwarded to my real account.

This service helps you identify how companies share your personal information. While writing this book, I encountered a service that required an email address before I could access any potential personal information about me on their website. I provided the email address of shady@nsa.33mail.com. I received an immediate email verification link at my personal email address that was forwarded by 33 Mail. One week later, I began receiving several spam messages from various clothing retailers. They were all addressed to shady@nsa.33mail.com. I now know that this web service shares their email

database with online marketers. In one click, I could block all future email from that address. You can use this technique to monitor how your information is shared. I recommend a unique email address through 33 Mail for every removal process mentioned in this book.

As a free user, you can reply to one message per day from the anonymous address that you created. This is still in beta, and not extremely reliable, but worth testing. If you reply to this message, it will be delivered to a unique email address only used once for each message. When 33 Mail receives your reply, it will forward your message back to the original sender. However, instead of your real email address being visible, the recipient will see your 33 Mail address.

I am excited to see this new service. I have been using it successfully for several weeks. While many social networks and other services have begun blocking addresses that end in notsharingmyinfo.com, I have found very few that are blocking 33mail.com. I encourage you to create, test, and maintain addresses through both services.

Blur (abine.com/index.html)

Blur is one of my favorite new privacy enhancing services. The service is available through a web-based login or through a dedicated mobile app. Blur offers a free trial that allows use for thirty days. Unfortunately, this trial does not include access to many of Blur's features. The options offered by the full version of Blur include password storage, password generator, masked email addresses, masked telephone numbers, and masked credit card numbers. This section will only discuss the masked email option while later chapters will outline the masked phone numbers and credit cards.

Masked email addresses allow you to use email addresses that will forward to your real address but appear randomly generated. An example of a Blur-generated email address is a049b2d21@opayq.com. Blur allows you to create as many of these email addresses as you wish. When you no longer desire to receive email from a given address, you have the option to turn forwarding off, similar to 33 Mail.

These “masked” addresses allow you to give out an email address that does not leak information about you and does not give up your “real” address This could be used as a starting point for an attack against you. It also allows you to create unique user names for each online account you have. Again, this greatly reduces your visibility and attack surface. More details about this premium service will be explained later.

Use Caution with Mail Forwarding Services

I use 33 Mail and notsharingmy.info extensively. However, you should approach these services cautiously. Using mail forwarding services gives these companies access to the content and metadata of your email. Because of this, I recommend never using these services in conjunction with your real name, email addresses that are personally tied to you, or for messages containing personal content.

Anonymous Telephone Number

Having an anonymous telephone number to provide to various sites and services that demand one is very important. Years ago, this would be difficult and expensive. Today it is easy and free. There are several services that will issue a telephone number to be used over the internet. This is called Voice Over Internet Protocol (VOIP). Some of these services have a small fee, and some are free and advertiser supported. One of the most common is Google Voice.

This free service will assign you a new telephone number in your area code and let you make and receive calls. This service is free but has many drawbacks. You must associate the account with an actual telephone number and email address. All of your incoming voice mail will be transcribed and analyzed. You will then see advertisements based on the conversation recorded by the service. I believe all of this is invasive. As a privacy advocate, I do not recommend daily personal use of the Google Voice service. However, it is the only stable free option currently available. It is adequate for the techniques described in this book.

However, the way that you create the account is very important.

Google Voice (google.com/voice)

Most users of Google Voice create an account on their home computer, provide their real name, associate their cellular telephone number with the account, and use the associated Google Mail account for all of their personal email. I will do none of that. You should have already created a Google Mail (Gmail) account. When you log into this account and navigate to google.com/voice, you will have the option to create a new telephone number. You will be prompted to enter a valid telephone number before you can choose your new number. This must be a number where you can receive a text message or telephone call in order to verify your access to the number. This can be tricky. You do not want to associate your real cellular or landline telephone with this service. If you do, your new "anonymous" number is not anonymous at all. Instead, you only need a telephone number where you can receive one telephone call. There are many options.

- ✓ Many hotels allow guests free unlimited incoming calls. If the hotel you are at provides a direct line to your room, you could use this. Google must be able to dial a ten digit direct number, and not dial an extension.

- ✓ Your place of work probably has several direct telephone lines that you have access to. You can tell Google to contact you at one of them.

- ✓ Your local library probably has a fax machine for patron use. The direct phone number of this device is likely written on the machine. These machines are usually set to not accept an incoming fax. Therefore, if it rings, you could answer.

Use your imagination and position yourself at a location that provides both wireless internet access and an incoming telephone line. You can use a laptop computer to complete the setup. Provide the telephone number that you have access to and allow it to call you. When you answer, you will be given a two-

digit code. Type that code into the Google Voice window that is requesting it. You have now activated your Google Voice account and can choose your area code and new number.

By default, Google will want to forward all incoming calls from your new number to the number associated with the account. In the settings menu, under the phones tab, uncheck any options for call forwarding. This will force any incoming calls to go straight to voicemail. You can create a custom voicemail message, but I recommend leaving the default generic message. In the "Voicemail & Text" tab, you can choose to have all messages forwarded to your anonymous email address. You now have a new telephone number that you can receive incoming calls and the caller can leave you a message. That message will be forwarded to your email inbox.

Blur (abine.com/index.html)

In addition to providing masked email addresses and a number of other services, Blur also offers masked telephone numbers. Only one number is available per account but it can be changed for a fee of $7.00. If you choose to use your Blur number for opt-out purposes, I recommend using it only for this and changing it once you have completed your opt-out journey. Blur will be discussed in greater detail in later.

Mailing Address

Most services, memberships, and publications that you sign up for are going to want a mailing address. Using your personal residence is one of the worst practices when trying to stay private. For much of this book, you will focus on removing any trace of your home address from several databases. Occasionally, you may need a real address where you can receive mail. I recommend a PO Box at your local post office. These are associated with your real name and personal address, but only the post office will have access to that information. It will not be passed on to any public databases. I like to have a post office box address available for various services such as utilities, medical, or any organization that needs to send a bill or invoice.

You can print an application from the USPS website or receive one in person at your local post office. A later chapter will discuss how to start sending all of your mail to your PO Box, and eventually no mail designated for you and your family will arrive at your residence. This may sound like overkill, but all of those magazines, coupon packs, and advertisements sell your information to many online services. You will never eliminate this information from the public internet until you stop receiving items at your home. The only mail that should continue to arrive will be generic items addressed to “Current Resident”.

Driver’s License Image

In order to complete the data removal process with some companies, they will want to verify that you are indeed the person requesting the removal. Most companies do this by demanding a copy of your driver’s license. Many of you are probably skeptical of this request, but there is no way around it. Fortunately, you can mask most of the personal content on the license before you send a copy.

The first step is to create a digital image of your license. There are two ways to do this. The easiest way is to use a digital camera or the camera on your cellular telephone to take a close-up image. Try to get good detail and fit the license perfectly into the border of the photo. An alternative to this method is to use a scanner connected to a computer. After you have created the image, use photo editing software to mask some of the information. For those of you that use Microsoft Windows, which is most of you, there is a free tool for this already installed. Click on the start menu, then “Programs”, then “Accessories”, then “Paint”.

This program will allow you to manipulate the digital image that you created of your license. The only information that the companies need from this image is your name, address, and date of birth. Therefore, you should give them nothing more. You could use the paintbrush feature of this program to mark over the additional information, but that looks messy and is more time consuming. Instead, use the “Shapes” tool to easily draw filled blank boxes around all other sensitive information. Mac users can execute the Preview application and use the Line Selection tool to block any sensitive data. Figure 3.01 shows an example of a masked driver’s license image.

Opt-Out Request Forms

You are now ready to prepare your generic Opt-Out Request Forms that will be used for submission to several companies. By creating one form that has all essential information, you will not need to create a new form for each company from which you want your information removed. I recommend using Microsoft Word for this, but you can use any word processing program you prefer. If you do not use Microsoft Word, you will need to save your document as a PDF file, which will be discussed later.

The first form will be referred to as the “Basic” form, which will contain the following information.

Date: This should be the date of the submission of the form.

Company: This should be the official company name that owns the database containing personal information.

Request: A brief statement identifying the request. I recommend “I request to have my name removed from your public and non-public databases. Here is the information you have asked me to include in my request.”

Name: Your full name as it appears in the online database. This should reflect any shortened or misspelled names as they appear online.

Mailing Address: Any addresses that appear in the database that you want removed.

Social Security Number: This should only be included when specifically requested. The few sites that demand this will be identified in this book.

Date of Birth: This will be necessary for all requests that require this form.

Direct URL(s) of personal information: This will be direct links to information that you find online that you would like removed from the internet. A “URL” is

the “Uniform Resource Locator”. It is the address of a web page. Examples of URLs are google.com,facebook.com/user/johndoe, and pipl.com/opt-out. It is the information that you type into the address bar to get to a specific web page.

Driver’s License / State Issued ID: This is a copy of the redacted image that you created in the previous step.

The second form that you should create will be referred to as the “Extended” form. This form will only be used for a small number of companies, and will not be necessary for everyone reading this book. These companies include data brokers such as Westlaw, Accurint, and LexisNexis. The data in these databases includes several pages of information about you including every place you have lived, every car you have owned, your SSN and DL number, all of your family member’s names and locations, your neighbor’s names and phone numbers, limited financial information, marriage and divorce information, court cases you are involved in, and much more. Law enforcement relies on these companies for information, but the data is not limited to the government. This information is also shared with businesses that are willing to pay for it.

The profile created about you includes information from both public and private sources. While the government customers get access to all of the information available, private businesses are issued a redacted view. This usually only removes a person’s Social Security Number and Driver’s License Number. The rest of the personal details are available to any commercial customer with a few bucks. This can include lawyers, private investigators, hiring firms, and anyone else that has an affiliation with a business. Most organizations pay a monthly premium for unlimited data requests about individuals. The wide scope of people that can access these personal details is disturbing to me. Removing your information from these databases is more difficult, but possible.

Since this data is much more valuable than public information from websites, the removal process is stricter. The companies that sell this data are bound by the rules of the Fair Credit Reporting Act (FCRA). All companies must allow people to have their information removed as long as the person requesting the removal meets any of the following criteria:

- ✓ The person is a judge, public official, or member of law enforcement;

or

- ✓ The person is the victim of identity theft; or
- ✓ The person is at risk of physical harm

At first glance, you may read this and think that you would not meet these requirements. The criteria is actually quite broad and will be explained later. The only instances that you will need this form will be during the removal processes explained in Chapter Eight. You will learn how to complete this form there and do not need this step completed until then.

Once your basic form is complete, save it and have it available when needed throughout the rest of the book. Each technique in this book that requires this form will explain which information to complete on the form and where to submit the completed form. Note that the printed version of the driver's license in this book masks the name, address, and date of birth in grey. This information should be visible on your copy. The information masked in white should also be masked on your version. Figure 3.01 displays my own form used during these techniques.

Facsimile (fax) Service (GotFreeFax.com)

Several companies demand that requests for removal from their databases be sent via fax. This outdated and wasteful technology is seldom used by the general public. Fortunately, several online websites assist with this function free of charge. I believe the best free service is Got Free Fax at www.gotfreefax.com.

When a section of this book instructs you to send a fax to a company, navigate to this site. Enter your name and new email address into the "Sender" section and the company details provided into the "Receiver" section. This should also include the subject line of "Data Removal".

The next section of this website will allow you to send a free fax using two different methods. The first method allows you to enter text directly into the site

and send that text. The second option will allow you to upload a document to be sent. You should use this second option to send the Opt-Out Request Form mentioned earlier. This site will only accept documents with a DOC or PDF extension. If you are using Microsoft Word, the DOC extension is usually the default. If your version of Word is newer that 2007, this default extension may be DOCX. You may need to open the form and select “Save as” and change the file type to DOC. If you are using a free word processor such as Open Office, you will have the option to save any document as either DOC or PDF.

Select the option to “Upload a PDF or DOC file to fax”. This will display a “Browse” button. Click on that button and select the document you created from the window that opens. In the section directly below this option, choose the “Send FREE Fax Now!” button. You will receive an email that will include a confirmation link. When you click this link, the fax will be delivered. Each time that this method is required in this book, you will have complete instructions on what information to include with the fax.

This chapter probably takes more effort on your part than any other chapter in the book. It is for good reason though. If you followed all of these steps, you are ready to begin eliminating your private data from the internet.

Date_____ Company_____

I request to have my name removed from your public and non-public databases. Here is the information you have asked me to include in my request:

Name: _____

Mailing Address: _____

Social Security Number *(If Required)* _____

Date Of Birth *(If Required)* _____

Direct URL(s) of personal information online:

http://_____

http://_____

Thank you for your prompt handling of my request. I have also included a redacted copy of my driver's license below to prove identity.

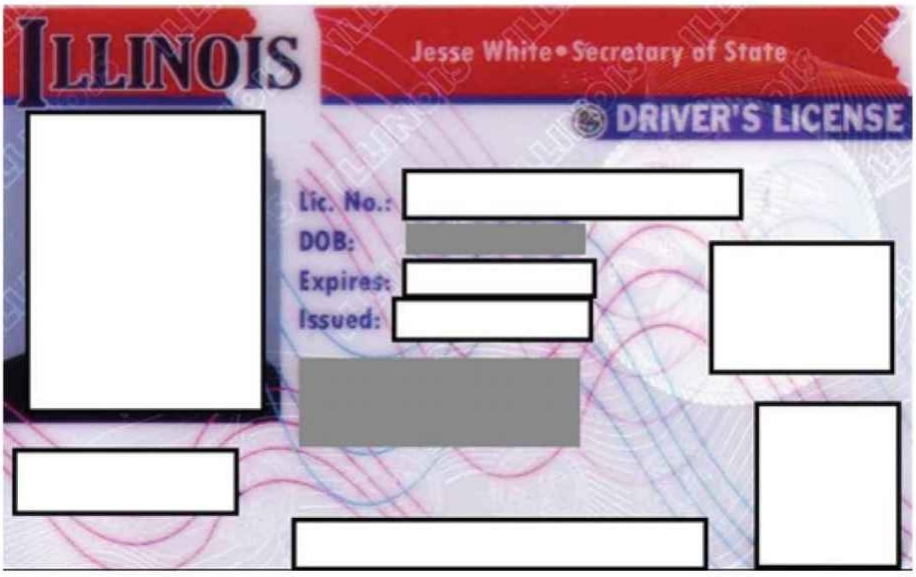


Figure 3.01: An example of an Opt-Out Request Form.

Chapter Four

Online Protection

Much of the private information that you share with various companies originates with your internet traffic. Before you begin the process of eliminating your data online, you need to properly protect any computer that you will use on the internet. Entire books have been dedicated to complete computer security. This chapter will focus on the core concepts that should be followed to stay help invisible. Some of these techniques can require a high level of technical skill. I have separated the chapter into three specific groups. The chart below should help you identify which group you fit in.

Privacy Level	Protection Level	Skill Level
Basic	The bare minimum of effort that anyone reading this book should perform. This provides basic protection to block a lot of personal data.	If you can point to the computer in your home, you will have no problems here. Knowing what operating system you have will help.
Intermediate	The next level of protection for true privacy seekers. This will be the suggested level for most readers that want to stop sharing personal details.	You know what a web browser is, the difference between Mac and Windows, and worry about the "cookies" on your computer.
Advanced	The highest level of protection designed for those that want to eliminate any unnecessary trace of personal information from leaving their computer.	You know how to boot your computer from a CD, you already clear out your cookies weekly, and you understand how an IP address is used.

Basic Protection

Too many computer users purchase a desktop or laptop, plug it into their home internet connection, and mistakenly believe they are ready to start browsing the internet. Within moments of starting the system, you are vulnerable to viruses, malicious software (malware), and tracking data. My book ***Personal Digital Security*** walks you through all of your options for configuring your systems and devices. Here, I will summarize the basics for Microsoft Windows users.

Antivirus

There are dozens of popular antivirus solutions for Windows based systems. Many are not free and can cost over $100 annually. Only free solutions will be discussed in this book. Antivirus programs run continuously and monitor all activity. This includes any time you open a document, launch a program, or download a file from the internet. The program scans all new files and

quarantines any files that are suspicious. It will usually then prompt you for action. There are two very important things to consider when configuring your antivirus program.

The first is to make sure that your program is receiving updates. I have seen computers that possess an expired version of premium software that is no longer receiving any updates. This is the same as having no antivirus software at all. The second important detail is to make sure you only have one antivirus program installed on the computer. This is a situation where more is actually less. If you have more than one antivirus program, they will battle each other for authority over your system. If you have an expired premium software package, such as Norton or McAfee, and you do not plan on renewing the service, you should uninstall it completely. If you currently have a paid or free version of premium software, and you have verified that it is functioning and receiving updates, you should leave it on the computer and disregard installation steps for the next program, Microsoft Security Essentials. However, if you believe, as I do, that some of these premium software packages slow your computer down, you may want to consider replacing your current program.

Windows 7

If you want to stick with Microsoft created security programs, Security Essentials is your only option. This free program is provided and maintained by Microsoft and will work on any version of Windows from XP through 7. This software is not included with any of these versions of Windows and must be downloaded and installed. The following steps will complete the installation.

- ✓ Navigate to: windows.microsoft.com/en-us/windows/security-essentials-download.
- ✓ Click on the “Get it now” button.
- ✓ Execute the downloaded file and allow the default choices.

If successful, you should see a green window when launching the program from either your start menu or the status bar in the lower right portion of your screen.

Other Antivirus Solutions

In the previous version of this book, I recommended AVG Antivirus. At the time, it was a great product. Since then, they have changed their privacy policy in a negative way. Basically, AVG states that they will collect data about your internet usage and overall computer activity. This data will be stored on their servers and they have the right to share this information. I can no longer advise anyone to use their products. While Microsoft has their own issues about collecting users' information, their products work well. There are numerous third party antivirus applications, and many of them are great. For most users, I suggest simply using the Microsoft solutions.

Windows 10

Many new computers now arrive with Windows 10 installed. This new operating system is very different than every other version of Windows. Windows 10 comes with antivirus software already installed. This software is also called Windows Defender, but should not be confused with previous versions of Windows Defender for older operating systems. The new software replaces Security Essentials and is free for all users of Windows 10. If your new computer came pre-configured with a trial edition of antivirus software, such as Norton or McAfee, you will need to uninstall the trial software before you enable Windows Defender. Personally, I recommend the free Windows Defender program for Windows 10 computers.

System Updates

Securing your operating system is vital to protecting your computer from online threats. Thousands of hackers are constantly scanning Internet Protocol (IP) Addresses looking for vulnerable computers that do not possess specific security patches. No matter which version of Windows or Mac OSX you use, even if the computer is brand new, you should apply security patches weekly. Most versions of Windows will conduct this patching automatically by default if you allow it. The following instructions will demonstrate how to make sure that your computer system is automatically updated when a new security patch is released. Your computer must be connected to the internet to download any updates.

Windows 7

Click on the “Start” button on the lower left portion of the screen. In the right column, click “Control Panel”. Click the last option, “Windows Update”. Click on “Change Settings” and review the options. For optimum results, make sure that all boxes are checked.

Click “OK” to close this window. If you made any changes, you may want to click “Check for Updates” to manually download any pending security updates for your system. If this automatic setting was disabled for some time, or you are setting up a new computer, it may take up to an hour to retrieve and install all of the updates. Many updates will require you to reboot your system. After reboot, you should check for new updates. After you have your system completely updated, you will probably only notice updates once a week. Your computer will conduct the updates automatically and finish the process upon restarting.

Windows 10

Open Windows Update by swiping in from the right edge of the screen (or, if you're using a mouse, pointing to the lower-right corner of the screen and moving the mouse pointer up), tapping or clicking Settings, tapping or clicking Change PC settings, and then tapping or clicking Update and recovery. Next, tap or click Choose how updates get installed. Under Important updates, choose the option that you want. Under Recommended updates, select the Give me recommended updates the same way I receive important updates check box. Under Microsoft Update, select the Give me updates for other Microsoft products when I update Windows check box, and then tap or click Apply.

This brings up a common question that I receive during my presentation. Many people ask whether they should turn their computer off at night or just leave it on all of the time. There are many different opinions on this, but I firmly believe that you should turn your computer off at night, or when it will not be used for an extended period of time. The reasons are listed below.

- ✓ Specific hardware in the computer, including the standard hard drive, has a limited life. Since it has moving parts, every standard hard

drive will fail eventually. The less time that your computer is on, the less time that the hard drive is spinning at 7200 revolutions per minute (RPM).

- ✓ When a computer is turned off, it cannot respond to digital attacks.

- ✓ Turning off your wireless router and internet connection device when not in use will provide even more protection.

- ✓ Turning the computer off when not in use will save energy.

Now that you have your Windows operating system updated and are receiving new security patches, you need to enable other software that will monitor your system for malicious software. I still recommend the default option of Windows Defender.

Windows Defender

If you are using Windows 7 or newer, you have an option called Windows Defender in your control panel. This is probably already turned on and this icon will open the settings. Unless the service is turned off, you need to do nothing. If the service is off, follow the on-screen instruction to activate the program. This program will continuously monitor the files on your computer and eliminate any malicious files that it identifies. While this is a great layer of protection against some malware, it is not a complete solution and provides no protection against computer viruses. For this, you will need a reliable antivirus program.

Mac OSX

The default configuration for the many versions of Macintosh OSX is to prompt you when an update to the operating system is available, but not to apply the update without your intervention. Visit the “App Store” within your “Applications” folder. Click on the “Updates” tab in the upper right of the screen. You will be notified of any available updates. Select the updates and follow the instructions.

Anti-Malware

At this point, you are probably asking yourself why you would need additional protection than the products already discussed. You may also feel that adding more protection is too difficult and you may want to abandon installing more programs. Unfortunately, there is no one program that will catch and remove all malicious software. In fact, if you encounter a program that makes this claim, it is probably a virus in disguise. I would avoid any product that guarantees to stop all intrusions. If you have successfully downloaded the programs that were previously discussed, they are now monitoring your system and you need to take no additional action. The following two programs in this section do not necessarily monitor your system at all times. They are present on your system and waiting to be executed.

Malware Bytes

After cleaning out any temporary and unnecessary files, I recommend the first scan for malicious files on your computer. Overall, you will use three individual programs to make sure that you have removed everything, but I believe the Malware Bytes is the best.

- ✓ Navigate to http://www.malwarebytes.org/ and select the “Download” option.
- ✓ This will forward you to second page to choose the version. Select “Download Free”.
- ✓ Execute the downloaded file and accept the default installation options.

After you have installed the application, you must execute it in order to run a scan. Malware Bytes (and the remaining applications in this chapter) do not run in the background as an antivirus program does. I recommend that you perform a scan at least once monthly. The following steps should be taken every time you run the program.

- ✓ Click on the “Update” tab and choose “Check for Updates”.

- ✓ If any updates are available, allow the program to install the updates.

- ✓ Under the “Scanner” tab, choose the default option of “Perform full scan” and click “Scan”. Choose the drives you want to scan. I recommend that you check the C drive and any other hard drives attached to your computer. The program will automatically scan your computer and remove any threats. You will receive a report at the end.

Spybot

Spybot is another application that will identify and remove malicious software and unnecessary files. You will probably notice that it will identify files that Malware Bytes missed. This does not mean that either product is superior to the other. Each of the products discussed in this chapter have unique strengths that allow them to repair issues that other programs miss. While there are hundreds of programs that will clean your computer, I believe that a combination of the products mentioned will cover all of your needs. To install Spybot, complete the following tasks.

- ✓ Navigate to http://www.safer-networking.org and click the “Spybot Free” link.

- ✓ Choose the option to download the free edition under the “Home Users” category.

- ✓ Execute the downloaded file and allow the default installation options.

Similar to the previous two programs, I recommend scanning your computer with Spybot at least once monthly. This can be on the same day that you scan with the other programs. I will later discuss the recommended order of events. To update and run Spybot, complete the following steps.

- ✓ Choose the “Update” button on the home screen. The updates will be applied automatically. Close the update window when complete.

- ✓ Click on “System Scan” on the home screen. Choose the “Start a scan” button and allow the program to analyze your system.

- ✓ When complete, click the “Show scan results” button to view all of the problems that were found. The items will all be selected and you only need to click “Fix selected” at the bottom to remove the threats.

CCleaner

CCleaner is one of my favorite programs ever created. It provides a simple interface and is used to clean potentially unwanted files and invalid Windows Registry entries from your computer. It was originally called Crap Cleaner, but I assume that someone in the marketing division demanded a better name. This software works on both Windows and Mac computers. The following steps will download and install the free version of the application.

- ✓ Navigate to http://www.piriform.com/ccleaner/download.

- ✓ In the “Free” column, click on the “Download” button to get the Piriform CCleaner version. This will ensure that you download the free version. The download should start automatically.

- ✓ Execute the program and accept the default installation settings.

After the installation completes, launch the program. You have several options under the Cleaner tab that will allow you to choose the data to eliminate. The default options are safe, but I like to enable additional selections. Figure 4.01 displays my choices. Clicking on the “Analyze” button will allow the program to identify files to delete without committing to the removal. This will allow you to view the files before clicking “Run Cleaner” to remove them. If you are running this program on a computer with heavy internet usage, you may be surprised at the amount of unnecessary files present. The first time you use this program, the

removal process can take several minutes and possibly an hour. If you run the program monthly, it will finish the process much quicker.

The Registry tab of CCleaner will eliminate unnecessary and missing registry entries. This can help your computer operate more efficiently. The default options on this menu are most appropriate. Click on “Scan for Issues” and allow it to identify any problems. This process should go quickly. When complete, click on “Fix Selected Issues” to complete the process.

The Tools tab provides an easy way to disable specific programs from launching when your computer starts. These programs can slow your computer down when they are running unnecessarily. Figure 4.02 displays four programs scheduled to launch when my computer starts. These can be found by clicking the “Startup” button in the left column. I have selected the Adobe and Java programs and applied the “Disable” button. They are now marked as “No” and will not launch the next time my computer starts. If I want to reverse this, I can select the entries again and choose “Enable”.

Use a better browser

Most people settle for Internet Explorer as a web browser, which is included with Windows operating systems. I do not recommend using that browser for safe browsing. There are many free web browsers from which to choose. They all have strengths and weaknesses. These browsers do not look much different from the browser you are currently using. My recommendation is the free Firefox browser.

Firefox (mozilla.org)

The Firefox browser has several features that are missing from some default browsers. It can be configured or tweaked for privacy and allows third party software called “add-ons” or “extensions” to be installed. These are small applications that work within the browser that perform a specific function. They will make private browsing much easier. Firefox also has some optional features that you can customize to enhance the privacy of your web browsing. Some of Firefox’s privacy features are enabled by default, however there are a few that

need to be configured.

With Firefox open, select “Tools” and then “Options” in the toolbar. This will open a new window with many options. The top row of menu options includes an icon titled “Privacy”. Selecting this option will display three categories of configuration options. The first section is titled “Tracking” and has only one option which is unchecked by default. Checking this option will prohibit some websites from tracking your internet usage. The next section, titled “History”, tells Firefox how much of the history of your internet usage that you would like it to store. I recommend the “Never remember history” option. With this selected, every time that you close the browser, it “forgets” your internet history. Launching the program will present a fresh session without any memory of the previous session. Finally, the last section titled “Location Bar” will instruct the browser on what information to store and display when a new website address is entered (“Bookmarks”). This way, when you type in a website address, Firefox will only look into your stored bookmarks for information about the site to navigate to. Figure 4.03 displays these custom options for this menu item.

When installing and executing Firefox, choose not to import any settings from other browsers. This will keep your browser clean from unwanted data. The extensions detailed here will include a website for each extension. You can either visit the website and download the extension or search for it from within Firefox. The latter is usually the easiest way. While Firefox is open, click on “Tools” and then “Add-ons” in the menu bar. This will present a new page with a search field in the upper right corner. Enter the name of the extension and install from there.

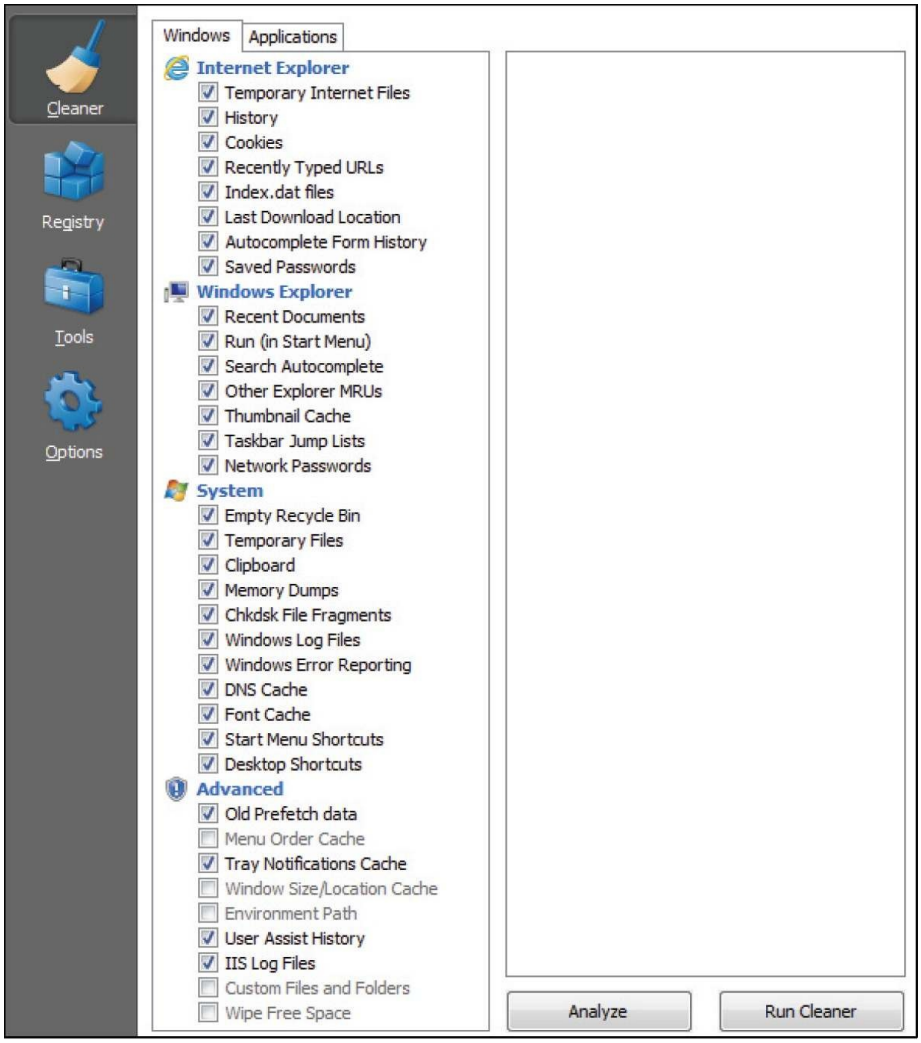


Figure 4.01: The CCleaner cleaning options recommended for most installations.

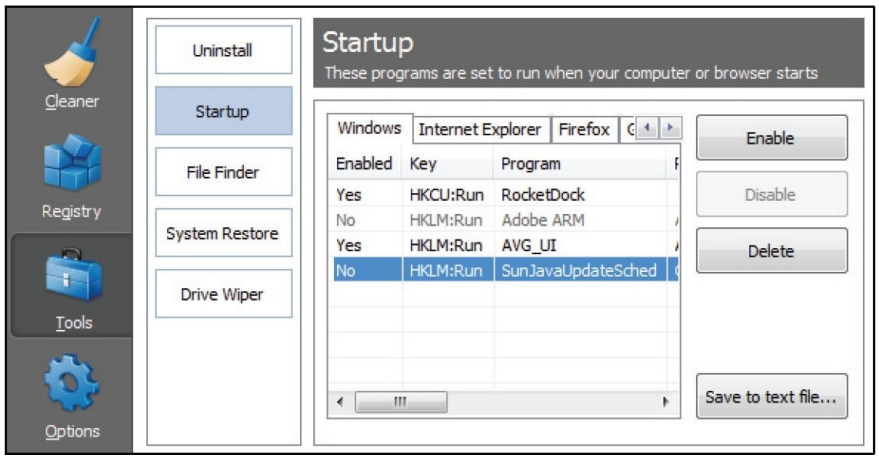


Figure 4.02: The CCleaner startup options with two services disabled.

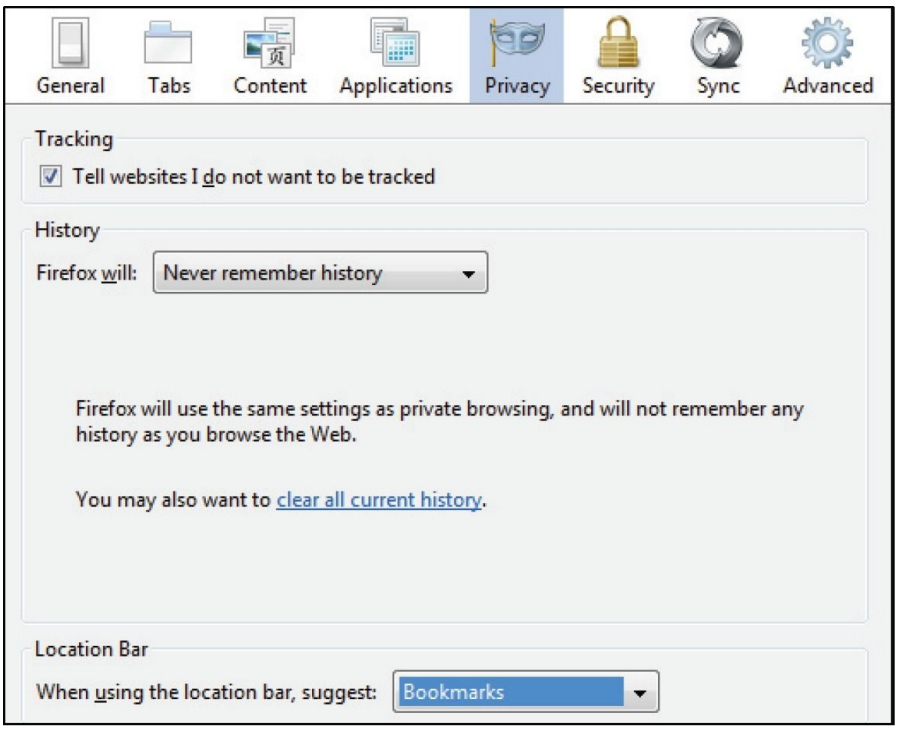


Figure 4.03: The Firefox Options menu.

Firefox Extensions

There are thousands of extensions available for Firefox. Some are helpful, some are worthless, and some are just fun. This chapter will discuss three of these extensions, Disconnect, Disconnect Search, and and AdBlock Plus.

Disconnect: Though I have used a number of add-ons over the years in an attempt to defeat tracking, the one I prefer now is Disconnect. Disconnect detects and blocks trackers and shows a graphic display indicating how many advertising, analytics, social, and content requests are made when you visit a site. It also shows how many of these are blocked and which ones are not. Disconnect also saves both bandwidth and time by not allowing advertising content to be served to you.

Though NoScript (discussed below) can help prevent tracking like Disconnect and may be considered redundant by some, Disconnect is a dedicated anti-tracking app. I believe what redundancy does exist between these two add-ons is necessary because NoScript frequently is too heavy-handed and will not allow a

site to work properly. In these cases, I have to allow the page (whether permanently or temporarily). When this occurs and a page is allowed to run, I still want some protections in place. Disconnect does not replace NoScript (and vice-versa), but they do complement each other well.

Disconnect Private Search: This is one of my favorite Firefox extensions. Disconnect Private Search can replace the default search engines in Firefox and route all of your searches through a "light" VPN via a Disconnect server. This allows you to search semi-anonymously because the search provider does not see from whom the search is originating. Additionally, if you set Disconnect Private Search as your default search engine, all your searches (whether from your homepage, Google.com, the address bar, or the search bar) will be routed through Disconnect Private Search.

When you search through Disconnect Private Search your search terms are sent to your preferred search engine and those are the results that are returned. If you don't like those results, there is a drop-down menu within in the search page that allows you to search through any of the other search engines supported by Disconnect Private Search: Bing, Blekko, DuckDuckGo, Google, and Yahoo. Disconnect Private Search will warn you that because they trust DuckDuckGo, search requests are sent directly to that search engine. I like Disconnect Private Search for the convenience of having five search engines immediately available through a dropdown menu.

Adblock Plus: This is a content-filter add-on that does an excellent job blocking advertisements. Once installed and running Adblock Plus requires no user interaction. Adblock Plus is available on the Firefox Add-ons page.

Intermediate Protection

The techniques explained here will involve a slightly higher understanding of technology. Anyone can apply these methods to their daily internet use and I encourage you to consider this next step in privacy protection.

NoScript (noscript.net)

This extension for the Firefox browser provides superior protection from malicious Java, Javascript, Flash, popups, and other web-based programming code. The default configuration of this software will block practically any script programmed to execute when you load a web page. This will include advertisements, tracking cookies, applications, and anything else that is not native to the display of the web page. The reason that this is listed in the intermediate area is because the protection can often block core content required to properly view the website. The following instructions will explain how to properly install and access NoScript.

- ✓ Within your Firefox browser, click on Tools and then Add-ons in the menu.

- ✓ In the search field, type NoScript and install the first result. Restart your browser and notice the new "S" icon in the upper left. Clicking this icon will present the NoScript menu for the website currently loaded.

Figure 4.04 displays the NoScript menu expanded while on a website. The extension identified and blocked five scripts from launching within this website. This includes Facebook data, advertisements, and tracking programs. Allowing these programs would have jeopardized your privacy by collecting data about you, your computer, your browsing history, and your Facebook profile (if logged in).

There are options within this menu if you want to enable scripts. If NoScript is blocking something on a website and is preventing it from displaying the content you want, use the following guide to correct the issue. I recommend taking action in the following order which starts with minor changes and ends with disabling NoScript completely from the website.

- ✓ Click on the "S" icon to launch the NoScript menu. Attempt to identify the blocked script that is desired. If you can identify the specific script, select "Temporarily allow" next to the script name. This will allow the script to load one time. However, the next time you load that website, the script will be blocked again. In Figure 4.04, clicking "Temporarily allow Facebook.com" would allow any

Facebook script within the website.

- ✓ If you decide that any allowed script should not run in the future, you do not need to take any action. If you want to block the script right away, you can click the “Forbid” option next to the script name.

- ✓ If you decide that the temporarily unblocked script should always be allowed, select the “Allow” option below the “Temporarily” option next to that script. It will now always allow that specific script on any website. This may be beneficial to always allow a desired login or social network.

- ✓ The “Temporarily allow all this page” option near the bottom of the menu will reload the current website and allow any scripts as if NoScript were not installed. This can be beneficial when you cannot access the desired website appropriately and do not know which script is the culprit.

- ✓ The “Allow all this page” option will always allow all scripts to run on the current website. This can be beneficial when you commonly visit a trusted website, such as your bank or other financial service. Enabling this setting will advise NoScript to never block scripts on that page.

- ✓ If you are currently only using trusted websites and are frustrated with NoScript blocking desired content, you can choose “Allow Scripts Globally”. This completely disables NoScript and you are not protected. You can reverse this action by selecting “Forbid Scripts Globally”.

If you choose to use NoScript, you may not need to use the Disconnect and AdBlock extensions mentioned during the basic protection section of this chapter. I believe that NoScript is a superior service and provides more protection. In exchange for this security, you sacrifice convenience in your daily internet browsing. I hope that you find this inconvenience worth the reward of a safer online experience. The following describes my NoScript settings.

- ✓ I have a default NoScript installation and configuration within Firefox. I block all scripts while browsing and searching the internet.

- ✓ If I encounter a website that I cannot view properly, and it is a reputable website, I will select the “Temporarily allow all this page option” for a single use allowance.

- ✓ The first time I connect to trusted websites such as my bank, financial services, email, or educational site, I choose the “Allow all this page” to permanently allow the scripts. This allows the security verification settings of the website to work.

- ✓ When I am conducting important business, such as financial transactions or creating accounts on business websites, I select “Allow Scripts Globally”. As soon as I am finished, I choose “Forbid Scripts Globally”. My individual settings are still maintained. This allows third party required services to run such as credential verification.

- ✓ Before navigating to any questionable website, I ensure that I am again blocking all scripts. This is vital when I am conducting online investigations.

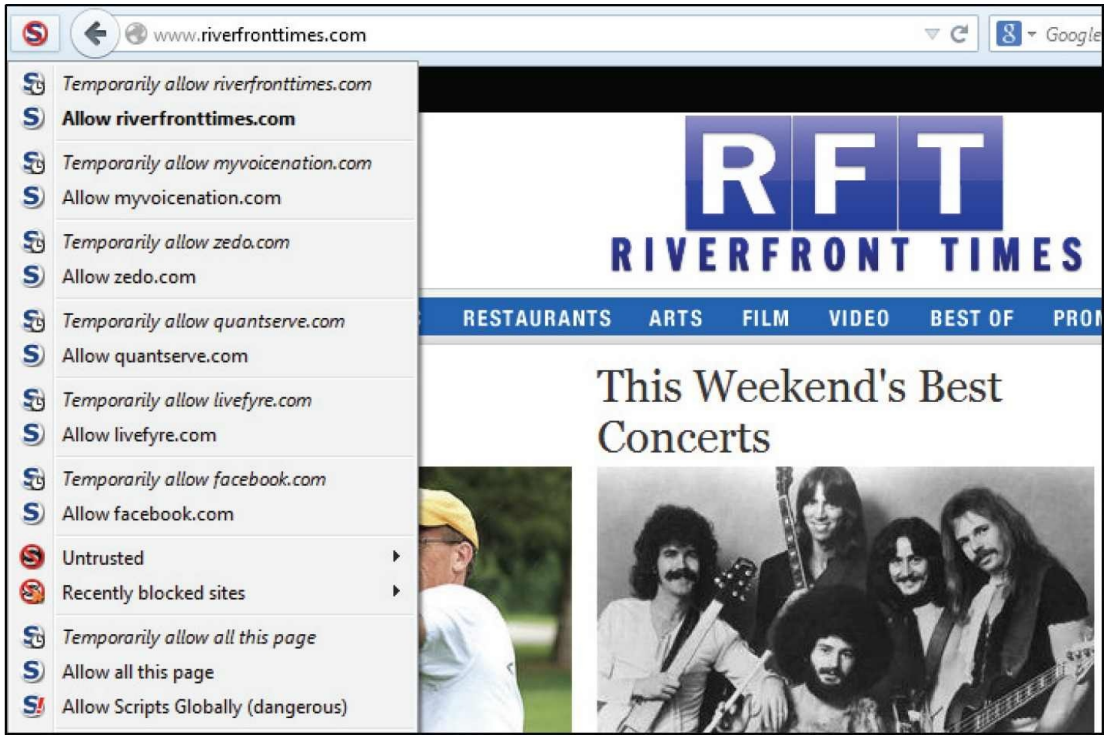


Figure 4.04: A NoScript menu for a loaded website.

Google Search Settings

Companies like Google make money from your internet browsing. Most of this revenue is from advertisements placed within your search results. You may have noticed that the ads that you see are directly related to your interests and shopping habits. This is not a coincidence. Google monitors your activity in order to deliver ads to you that you are likely to click. Some of this is based on cookies downloaded to your computer and some is from your search history.

If you use Google's free email service Gmail, you are targeted even more. Google scans through each email to deliver ads that are relevant to your conversation. While this tactic provides a great business strategy, many feel that it is intrusive. It is impossible to use Google's free services without giving them some of your information. However, completing the following steps will disable some of the most intrusive methods conducted against you.

- ✓ Activate Google Opt-Out by visiting the website www.google.com/ads/preferences/plugin. Click on "Download the

advertisement cookie opt-out plugin". Depending on your browser, the installation method will vary. This will install a small file that will prevent a company called DoubleClick from installing files that monitor your activity. DoubleClick is the company that Google relies on for this type of data collecting. This file will not be deleted when you manually clear your cookies or when you use a program to clean up your computer.

✓ Turn off Google's web history. This service archives all of your Google search activity. To view this history and settings, navigate to www.google.com/history. You will need to be logged into your Google account, such as Gmail, in order to see this page. Once logged in, click on the gear icon and select "Settings". If desired, check the box to include history from other web and app activity, and then click the "Pause" button. In the next popup, click the "Pause" button. Go back to "Manage History" to manually delete any searches made up to this point. Click on the gear icon and select "Remove Items". From the drop down menu, select "from the beginning of time" and click the "Remove" button. This will stop Google from capturing your search history. Figure 4.05 displays these options as well as the interactive calendar that will show your search history. Parents that want to monitor their children may want to leave this enabled.

✓ Opt out of Google's Ad Preferences. While logged into your Google account, navigate to www.google.com/ads/preferences/. Click on the "Opt out" button which will stop the interest based ads from appearing.

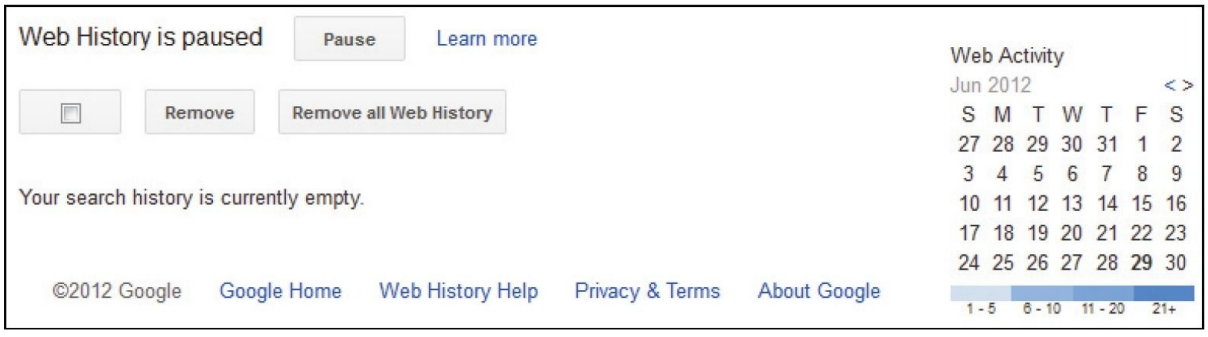


Figure 4.05: The Google Search History settings page.

Microsoft Search Settings

Microsoft has their own rules for their delivery of advertisements to your desktop. Disabling customized ads based on your internet history can be accomplished on the website at https://choice.microsoft.com/en-us/opt-out.

Choose the option “Off” within the box “Personalized ads in this browser”. This will not stop you from seeing advertisements from Microsoft’s services. However, these ads will be more random and not based on your internet activity. If you are signed into a Microsoft account, such as one of their email services, you can disable this personalization across all browsers. Finally, selecting the “Data Dashboard” on this page will allow you to see the data about you that Microsoft uses for advertisement delivery.

Advanced Protection

If you have reached this point of the chapter and you still have an appetite for more online privacy, this section will take you to the next level. These techniques are not recommended for everyone. Familiarization with computer hardware and software will be required.

Virtual Private Network (VPN)

Virtual Private Networks (VPNs) provide a good mix of both security and privacy by routing your internet traffic through a secure tunnel. The secure tunnel goes to the VPN’s server and encrypts all the data between your device and that server. This ensures that anyone monitoring your traffic before it reaches the distant server will not find usable, unencrypted data. Privacy is also afforded through the use of a distant server. Because your traffic appears to be originating from the VPN’s server, websites will have a more difficult time tracking you, aggregating data on you, and pinpointing your location.

Virtual Private Networks are not a perfect anonymity solution. It is important to

note that VPNs offer you privacy, not anonymity. The best VPNs for privacy purposes are paid subscriptions with reputable providers. There are several excellent paid VPN providers out there and I strongly recommend them over free providers. Free providers often monetize through very questionable means, such as data aggregation. This compromises one crucial benefit of a VPN: privacy. Paid VPN providers monetize directly by selling you a service, reputable providers do not collect or monetize data. Paid providers also offer a number of options that will increase your privacy and security. I currently endorse PIA as my trusted VPN. I will always maintain a direct link to the most affordable subscription to PIA on my “Privacy” page on both of my websites. The current rate for their service is $39.95 per year. This includes unlimited use and connection for up to five devices. I am not paid to mention them and I receive no free service. I happily pay yearly.

My VPN policy is quite simple: Any time that I am connected to the internet from my laptop, desktop, or mobile device, I am connected through my VPN. I then know that my internet traffic is encrypted and originating from an IP address not associated with me. I never deviate from this policy. I believe that every reader should consider a paid VPN.

Tor

Tor, an acronym for the onion router, is a network and a software package that helps you anonymously use the internet. Specifically, Tor hides the source and destination of your Internet traffic. This prevents anyone from knowing both who you are and what you are looking at. Tor also hides the destination of your traffic, which can circumvent some forms of censorship. Tor has been in development for many years and is very stable and mature. It is regarded as one of the best privacy tools currently in existence and it does not cost you anything.

Tor encrypts the data you send across the Internet in multiple layers, like an onion. Then it sends that data through multiple relays, each one of which peels a layer off the onion, until your packet leaves the final relay and arrives at its destination. This is called 'onion routing' and it is a fantastic method for keeping privacy on the web. Proper use of tor can be one of the best ways to ensure your browsing will remain anonymous.

For the purposes of a simple and incomplete explanation, consider the following to describe the actions of Tor. You connect to a Tor computer which routes your internet traffic through several other computers. This traffic is then sent to the "web" and returned to you through the same route. These computers are often in other countries and the traffic is encrypted. When you navigate to google.com, Google actually receives the request from another computer, in another country, from another IP address. Therefore, Google does not know who you are, where you are, or what other actions you are performing on other websites. Your IP address assigned to you from your internet service provider (ISP) is not disclosed to the websites that you visit.

The easiest way to apply this security is to use the Tor Browser Bundle. It is a version of Firefox that comes preconfigured with Tor. It is set up to use Tor the right way so that you will avoid a lot of the common pitfalls that can pierce your veil of anonymity. The following steps will help you download, execute, and properly browse the internet anonymously with Tor.

- ✓ Navigate to torproject.org and download the Tor Browser Bundle.

- ✓ Execute the downloaded file. This will extract all of the files necessary for the bundle. This software is "portable" and is not intrusive into your operating system. All of the settings are contained within the folder where the software exists. After the extraction is complete, allow the software to launch.

- ✓ You will receive a Tor Network Settings window that will configure the appropriate settings for your situation. Most users will select the first option which will connect you directly to the Tor network. The second option is only for advanced users that are behind a proxied or censored connection. Click the "Connect" button to launch your Tor session.

- ✓ You should receive a "Congratulations" notification when you have successfully connected. You can now use this browser for anonymous online activity.

This phenomenal layer of security does not come without costs. Your overall internet experience will likely be somewhat slower. However, the speed of the Tor network has increased substantially over the past couple of years. Some websites that you visit will detect that you are coming from a Tor connection and may refuse whole or partial service. Several websites that require an account to access content, such as Gmail, Facebook, and others, will often require additional steps in order to create or access an account while connected through Tor. Many will require a valid telephone number when detecting Tor connections. This is likely due to abuse of the Tor network by cyber criminals.

Tails

The Tor bundle will provide adequate privacy protection for the majority of users. Because Tor is installed on your computer within your operating system, there can still be vulnerabilities within the data stored on the computer. Your operating system possesses many details about your computer use and retains a record of further actions that you take. You would need to use a brand new computer every day and destroy the last used system in order to stop this type of vulnerability. The Tails live system provides a better solution.

Tails is a live operating system that you can start on almost any computer from a DVD, USB device, or SD card. You could use this operating system without a hard drive present in the computer. When using the DVD option, absolutely no details of your internet session are saved. It ultimately preserves your privacy and anonymity by routing all connections through the Tor network. Further, it leaves no trace on the computer you are using unless you ask it explicitly. It will also use state-of-the-art cryptographic tools to encrypt your files, emails and instant messaging. The following steps will help you launch your own private Tails system from DVD.

- ✓ Navigate to tails.boum.org and download the latest version of Tails ISO image.

- ✓ If using a Windows computer, right-click on the ISO image and choose “Burn disc image”. Select your DVD recorder and select “Burn”.

- ✓ If using a Mac OSX computer, launch Disk Utility from Applications-Utilities-Disk Utility. Insert a blank DVD and drag and drop the ISO file to the left pane in Disk Utility. Select the ISO file and click on the Burn button in the toolbar.

- ✓ If you are using Linux, you likely already know how to burn an ISO image.

- ✓ Put your new Tails DVD into the DVD drive and restart the computer. You should see a welcome screen prompting you to choose your language.

You can now perform basic internet tasks such as web browsing, email, and instant messaging. Your activity is only being stored in the computer's memory (RAM) and disappears when you shut down the computer. If you find this limiting and inappropriate for daily use, consider the following option for a virtual machine.

Virtual Machines

I currently use virtual machines every day. These are full computer operating systems that can be launched on top of your current operating system. The activity performed within a virtual machine is not associated with the main operating system of your computer. If you become infected with a virus or malware in a virtual machine, it does not infect your main operating system. These are often referred to as "sandboxes" that allow you to play inside of them without risk to your important data on your main computer. I will describe how I use virtual machines.

When I am conducting an investigation on the internet, I currently use a Windows 7 virtual machine while on a MacBook Pro laptop. If anything goes wrong during the investigation, my laptop is not compromised. This is not limited to viruses and malware. A website might capture details from my computer which could identify me. A virtual machine helps protect you in several ways.

- ✓ A virtual machine can use a full version of Windows. This can be beneficial because you can install any software that you need for daily use such as Microsoft Office, Adobe products, or custom browsers. Additionally, this avoids the learning curve involved with Linux based operating systems such as Tails.

- ✓ At the end of a session on a virtual machine, you can choose to delete any changes made to the system. This would eliminate any details that were left behind from your internet activity.

- ✓ You can possess multiple virtual machines for various operating systems. You can also have several copies of the same operating system that can be used for different purposes.

- ✓ Using a fresh operating system every time ensures that excess details about you and your activity are not visible to any websites or services.

- ✓ In the event of a virus or corruption that causes the system to not function, you can either return to a previous state or delete the entire virtual machine and start over.

Your need for virtual machines will vary from mine. You should create only those machines necessary for daily use. This may just be one machine with Windows or Tails that you use when you want to be private or have additional protection. I encourage you to attempt at least one virtual machine. Before I can explain the process, virtual machine software must be chosen.

There are many choices for virtual machine software. Most are commercial and cost money for a license. Some only work on specific operating systems, such as Parallels for Mac OSX. For the purposes of this book, I will explain how to use Virtual Box. This software is free and works on Windows, Mac, and Linux. The following steps will help get you started. These are simplified instructions and an understanding of operating systems will be required to complete this process.

- ✓ Navigate to www.virtualbox.org/wiki/Downloads and download the

appropriate version for your operating system. Install the downloaded file with the default options.

- ✓ Execute the software and click “New” at the top of the window to create a new virtual machine. Default configuration options are usually sufficient for most systems. You will need a valid installation disc and license for the operating system that you choose. Complete the installation process and refer to the Virtual Box website for troubleshooting.

- ✓ Once you have your virtual machine running, configure any custom settings. This may include software installation such as office suites or custom browsers and extensions. Do not conduct any web browsing yet. You want to keep this system clean.

- ✓ When your virtual machine is configured the way that you want it, create a snapshot. Click on the menu then select “Take Snapshot”. Provide a name and description to help remember the configuration. Your name might be “Windows 7 Pro” and the description might be “Clean install with Microsoft Office and Firefox”. You now have a recorded point in time that you can revert to if necessary.

- ✓ The purpose of creating a snapshot is so that you can go back to a particular state. In this case, we want to return to the state that existed just after we installed the operating system. Any time that you shut the virtual machine down, you can now revert to the snapshot that was created right after the install of a clean image.

- ✓ When you want to revert to a snapshot, select your virtual machine from the list and switch over to the snapshots view. Here you will see a list of the various snapshots you have taken. To restore to a snapshot, simply right click on it and choose “Restore Snapshot” from the context menu. You have now eliminated any data written to the virtual machine since the snapshot was taken.

Now that you have a basic understanding of virtual machines and snapshots, I

will explain how I use them on a daily basis. I currently use VMWare Fusion as my virtual machine software. It is not free, but I find it to be superior for my needs. I have five virtual machines installed and configured on my laptop.

Windows 7 Demonstration: I use this standard installation of Windows 7 during all of my presentations and training events. It is configured with all of the software that I need and has a snapshot of the image before I performed any demonstrations with actual data. When I turn it off after use, I revert to the snapshot.

Windows 7 Working: This updated and patched copy of Windows 7 opens any Windows only applications that I may need. I do not conduct any investigations on this image and do not expect total privacy. This is ideally for official business.

Windows 7 Investigations: This machine has minimal software installed. It possesses a custom version of Firefox which has many extensions that I use while browsing. Reverting to the snapshot after each session eliminates data about the investigation that I was conducting.

Tails Privacy: This is a standard installation of Tails as described with the DVD option earlier. Since my laptop does not have a DVD drive, and I find booting from USB too slow, this option works best for me. I always revert to the original snapshot after every use.

Windows 7 Privacy: I use this machine when Tails is not appropriate for my work. It has the Tor Browser as well as a custom Firefox browser with NoScript. It has also been configured to eliminate as much tracking as possible. This is not as secure as Tails, but much more user friendly. It suffices for the majority of my private browsing.

This selection of virtual machines will be overkill for most users. Much of my need for all of this is a combination of paranoia and enthusiasm for technology. You may also find that possessing multiple isolated operating systems can become addictive.

Chapter Five

Credit Companies

Credit companies collect a lot of information about you. They obviously know your name and personal details. Since they are providing you with a line of credit, they are entitled to know where to find you if you do not pay them. Unfortunately, they do not keep this information to themselves. They share their data with other creditors and various data mining companies.

Earlier, I mentioned an experiment that I conducted with a secondary credit card in a different name. The only company that I provided with this new name was my credit card company. After a few days, I requested my personal data from Thomson Reuters (CLEAR). This report included the new name as an alias to me. It identified my address as being used by this “person” and associated the name with my activities. This same report is available to anyone that has an account with one of the data mining companies. This report would cost under $6.00.

My point is that anyone can track you on the internet through your credit. The following methods will not replace the privacy of cash, but will eliminate much of the information available to the general public. This chapter is important for other concerns besides privacy. These methods will offer a new layer of security to protect you from identity theft and fraud.

Credit Opt-Out (optoutprescreen.com)

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. 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 this website, you may request to opt-out from receiving these 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.

- ✓ Navigate to optoutprescreen.com and click the button at the bottom of the page labeled “Click Here to Opt-In or Opt-Out”. On the next page, choose the second option of “Electronic Opt-Out for Five Years”

- ✓ Complete the online form and click “Confirm”. You will receive an immediate confirmation. This action will need to be repeated every five years.

Fraud Alert

A fraud alert is an action that you can take to protect your identity from being used by criminals for financial gain. You can place an initial fraud alert on your credit report if you think that you have been the victim of identity theft. This is a good idea if you see any suspicious activity on your credit report. It can also be used if your wallet or purse has been stolen, if you've been a victim of a security breach, or even if you revealed too much personal information online or over the telephone. A fraud alert means that lenders must take extra precautions to verify your identity before granting credit in your name.

Anyone can place a 90-day initial fraud alert in their credit report. This alert can be renewed in 90-day intervals indefinitely. To request the alert, you need to contact only one of the three credit bureaus. The chosen bureau will notify the others. The following links forward to the online forms to request a fraud alert. While you only need to complete one of these, I recommend completing all three

if you are a victim of identity theft. In my experience, Experian provides the smoothest process. If you decide to pursue a credit freeze, which will be discussed in a moment, do not complete the fraud alert process.

- ✓ Experian: https://www.experian.com/freeze/center.html
- ✓ Equifax: https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp
- ✓ TransUnion: https://fraud.transunion.com/fa/fraudAlert/landingPage.jsp

The alert should be activated within 24 hours. You should receive a confirmation in the mail within a few days. If you do not receive this confirmation within one week, place another alert. When activated, your name will be removed from all pre-approved credit and insurance offers for two years. Instructions for removing the fraud alert will be included with the documentation sent to you via postal mail.

You can also obtain an extended fraud alert which stays on your credit report for seven years. To qualify, you must provide a police report or other official record showing that you've been the victim of identity theft. You will receive two free credit reports from each of the credit bureaus every 12 months in addition to the free copies anyone can obtain yearly.

Fraud alerts are not fool proof. A lender can see the fraud alert when a query into your credit is conducted for the purpose of opening a new line of credit. When the lender observes this alert, the lender should contact you by phone to verify that you really want to open a new account. If you are not reachable by phone, the credit account should not be activated. However, a lender is not required by law to contact you even if you have fraud alert in place. Many criminals that will open new fraudulent accounts will seek friends and family that are associated with lending companies to process the request. When this happens, the fraud alert does nothing. Most criminals will not attempt to open an account with a reputable institution that would acknowledge the fraud alert and take extra precautions. If you would like to have real credit protection, you should consider

a credit freeze.

Credit Freeze

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, usually free, and reversible.

A credit freeze, also known as a credit report freeze, a credit report lock down, a credit lock down, a 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 the three big credit bureaus (Equifax, Experian, and TransUnion). The credit freeze locks the data at the consumer reporting agency until an individual gives permission for the release of the data.

Basically, if your information stored by the three 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. If someone decides 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, even yourself, 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.

The first step will determine whether your credit freeze will cost you any money. The fee for the freeze is $10 for each of the three bureaus. While this is well worth the protection, most states have a law that entitles identity theft victims a

waiver of this fee.

Currently, each of the three credit bureaus will voluntarily waive this fee for victims of identity theft. A large portion of this book's audience has had some type of fraudulent financial activity. This may be an unlawful charge to a debit or credit card or something more serious such as someone opening an account in your name. If you have had any fraudulent charges or activity, contact your local police to obtain a police report. Request a copy of the completed report including the case number.

Complete three packets that will be sent by certified mail. One will go to each of the three credit bureaus. Each packet will include the following:

- ✓ A letter requesting the credit freeze including the following information:

Official Request
Full Name
Full Address
Social Security Number / Date of Birth

- ✓ A copy of your police report if you have one.

- ✓ A recent pay stub or utility bill.

- ✓ A photocopy of your driver's license or state identification.

Send this packet to each of the following credit bureaus:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348

Experian Security Freeze
PO Box 9554

Allen, TX 75013

TransUnion
Fraud Victim Assistance
PO Box 2000
Chester, PA 19022-2000

If you do not have a police report and do not want the $10 fee waived, you can complete the entire process online at the EACH following three sites:

- ✓ Equifax: https://www.freeze.equifax.com
- ✓ Experian: experian.com/freeze/center.html
- ✓ TransUnion: freeze.transunion.com

The following is an example of a TransUnion credit freeze request.

TransUnion
Fraud Victim Assistance Department
PO Box 2000
Chester, PA 19022-2000

January 1, 2016

To whom it may concern,

Please accept this letter as an official request for a Security Freeze on my TransUnion credit file. Per your instructions, I have included a photocopy of my driver's license and recent pay documentation. Below are my details.

John Patrick Doe
1234 Main Street
Chicago, IL 61234

321-54-9876
December 1, 1980

I further request waiver of any fees due to my recent status as an identity theft victim in the State of Illinois. I have attached a photocopy of my police report.

Within a few weeks, sometimes sooner, you will receive a package from each of the bureaus confirming your credit freeze. This confirmation will include a PIN number that you need to keep. This number will be required if you ever want to temporarily or permanently reverse the credit freeze. After sending my requests via certified mail, and receiving the confirmation of delivery, I received a response from TransUnion within three days, Equifax within four days, and Experian within eight days.

If you want to reverse the credit freeze, you can do so online at the previously mentioned websites. A temporary reversal would be done to establish new credit such as a credit card or loan. Be sure to generate this temporary reversal prior to the loan request, otherwise your loan may be denied. A permanent reversal will completely stop the freeze, and your account will be back to normal.

Beginning in 2015, I also started recommending establishing a credit freeze with Innovis. If you have had a credit freeze in place for at least three years, this may not be mandatory. However, my opinion is that we should all take advantage of all protections provided to us. The method is the same and you should submit your letter to the following address. You can also establish the freeze online for free at Innovis' website located at www.innovis.com/personal/securityFreeze.

Innovis Consumer Assistance
PO Box 26
Pittsburgh, PA 15230-0026

Unless you are constantly opening new lines of credit or using your credit to purchase real estate often, I highly recommend a credit freeze. It is the most effective way of stopping people from using your identity for financial gain.

Lately, people are reporting that their under-age children are becoming Identity theft victims. A freeze could be applied to them as well. Generating a credit freeze on your child now will protect them until you request removal. This could protect your children from the temptation in high school and college to open new lines of credit.

After your credit freeze is in place on all three credit bureaus, you may want to test the system. In May of 2013, I decided that I was overdue for a test of my own credit freeze. The following are details of what I had to go through while attempting to obtain a new credit card with an active credit freeze in place.

May 27, 2013: I navigated to a website that was offering a great rewards point bonus for new members of a specific travel credit card. It was a very legitimate company that I have held credit with in the past. Even though I had a credit freeze in place, I thought that this company may use my previous relationship as a way around the freeze. This seemed like the best company to test my freeze with. I completed the online application and was told that I would receive an answer via postal mail soon.

May 29, 2013: I received a letter from the credit card company stating that they could not offer me a card. They advised that I had a credit freeze in place and that I would need to remove the freeze before my application could be processed. They identified TransUnion as the credit bureau that they ran my credit through. The freeze worked. This would stop the majority of criminals from accessing your credit. In order to continue the test, I contacted TransUnion and conducted a temporary credit freeze removal over the telephone. It was an automated system and I only had to provide the PIN provided earlier.

May 30, 2013: I contacted the credit card company via telephone and advised them that the credit freeze had been removed and that I would like to submit my application again. I was placed on hold for a few minutes. The representative stated that she could still not offer me the card. While the freeze had been removed, there was still an extended alert on my credit file and there was not a telephone number for me attached to the account for verification. Basically, TransUnion automatically added this extended alert to provide another layer of protection when a freeze was ordered due to fraud. The representative advised that I should contact TransUnion. I contacted them and was told that I should

add a valid telephone number to my credit profile. Before I was allowed to do this, I had to answer four security questions about historical credit accounts, addresses, vehicles, and employers. After successfully answering these questions, I was able to add my cellular number to my account. I was told the changes should take place within 24 hours.

May 31, 2013: I contacted the credit card company and advised of my actions taken. She advised that she would not be able to pull another copy of my credit for 14 days. This was policy and there was no way to work around this due to the fraud protection rules in place.

June 15, 2013: I contacted the credit card company again and requested a new pull of my credit report. The credit freeze was still temporarily disabled until the end of the month. The new credit request was successful, and the representative could see the extended alert and a telephone number for contact. She placed me on hold while she dialled the telephone number on file. My cellular phone rang and she verified with me that I approved of the new credit request. I approved and switched back to the other line with her.

June 19, 2013: My new credit card arrived.

This was an interesting experience. I had never tested the system with the intent of actually receiving the card. I had occasionally completed credit card and loan offers in the past for the purpose of testing the freeze, but I was always denied later in writing. This enforces the need to have a current telephone number on file for all three credit bureaus. This entire process took just over two weeks. Any criminal trying to open an account in my name would have moved on to someone else. This same chain of events would have happened if I were trying to buy a vehicle, obtain a personal loan, or purchase real estate. Even routine tasks such as turning on electricity to a home or ordering satellite television service require access to your credit report. A credit freeze will stop practically any new account openings in your name. While I became frustrated at the delay in obtaining this card, I was impressed at the diligence of the credit card company to make sure that I really was the right person. My credit is now frozen again and I am protected at the highest level.

Credit Options

There are some techniques regarding credit cards and lines of credit that you can apply to further protect your privacy and security. Credit companies do not promote these methods because the actions make it difficult for them to make more money from you. You may get resistance as you apply these techniques, but do not give up. You have every right to control your information.

Unused Accounts

When you obtain your free credit report as outlined earlier in this chapter, you should pay special attention to each line of credit. If you observe an old account that you have not used in years, consider closing the account. Usually, these dormant accounts do not cost you any money, but they do not help you either. This open account contains your personal information that can be sold and traded to other organizations.

Closing unused accounts will generally not affect your credit score. The only time this would apply is with your oldest credit account. One way that your credit score is determined is by the amount of time that you have had a line of credit in good standing. If you have had an unused credit card for ten years, that would help your credit score. If you close this account, and your next oldest account is two years, this may hurt your credit score. If you have any open account that is older than the accounts you are closing, your score should not be negatively affected.

Closing these unused accounts will also add security to your credit. Any accounts that you have open make you vulnerable to identity theft. The fewer accounts you possess; the fewer accounts can be compromised. Criminals often target dormant accounts that may not be watched as thoroughly as current accounts. Having multiple unused accounts can make it difficult to monitor for unauthorized transactions.

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.

Account Information

Credit companies share your home address to other companies. I highly recommend changing your address with your credit companies to your post office box or commercial mail receiving agency (CMRA). These mail drops can include commercial chains such as The UPS Store or locally owned mailing shops. This can be done by calling the number on the back of the card, but I suggest completing the process online. Calling the company and giving them the information may not help. The operator may simply add a new address to the account and not actually change the address of the account. If you have a login to access your account online, there should be an option to update your account. You then want to change your mailing address. If you do not have online access to the account, you can request access through your credit company’s website.

Secondary Credit Card

Credit card companies will issue additional cards at your request. These cards 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. Any time the secondary card is used, it is processed as if the original card had made the purchase. Since the secondary card is part of an account that has already been verified, there is no verification process to obtain the additional cards.

To request an additional card, 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. 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 as explained previously. I recommend confirming that the new address is active before ordering additional cards.

Many readers of the first edition of this book reported difficulty in obtaining a secondary card from traditional banks, such as Bank of America or U.S. Bank. I have found this technique to work best with traditional credit card companies. I have had great success, even recently, with several Chase cards. This technique will usually not work with debit cards.

There are a few ways that you can take advantage of this additional card. I have a credit card in an alternate name that I created for this single purpose. I keep the card with me next to my card with the same account in my real name. I now have a choice of which name to use when I make a purchase. I try to pay with cash whenever possible, but many scenarios exist where cash is not accepted. The following are examples of how this technique can keep your personal information private.

Hotels

Obtaining a hotel reservation is very difficult without a credit card. Some 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 scanned. This collects the data about the cardholder and attaches it to the sale. There are two main reasons for applying this technique 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 travelled 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.

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 conversation 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, Laura 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 call that gets the confirmation will identify where you are staying. A more high-tech approach could be conducted through the hotel's wireless internet. Many hotels require you to log into 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 you are staying at, but exposes the room number you are in. This can be a huge security concern.

You can use your new alternative name to create your hotel reservation. Since

you are not committing any type of financial fraud, this is legal. You will be providing your legitimate credit card number and will pay the charges through your credit statement. Upon arrival at the hotel, hand this card to the receptionist. You may 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 this does not work, have your travel partner show identification to meet the requirement. This information will most likely not be added to the reservation. I recommend persistence that you do not have an ID. Very few hotels will turn down a paying customer with a credit card in hand. I find that being polite and understanding always works better than acting agitated.

In 2014, I encountered a hotel chain that has made it absolute policy that the customer supplies both a valid credit card and photo identification in order to rent the room at check-in. I have found that the following two scenarios bypass this requirement almost every time.

First, create a rewards card with each of the hotel chains that you plan to use. When I check in, I immediately give both my credit card (alternative name) and my rewards card (also in my alternative name). Since I travel often, and I have an elevated status on my rewards card, I have encountered no resistance upon check-in. If I detect a stubborn receptionist that appears determined to follow the corporate rules, I will act like I am in the middle of a very important call on my cell phone. Usually, the receptionist will continue with the process just to get rid of me.

When I arrive at a hotel, I always hold the door open for anyone else entering and allow them to check in first. This is not me being polite, it allows me to determine what resistance I will be up against when it is my turn. Knowing the attitude of the employee may aid you in creating the most appropriate pitch.

If the previous trick does not work, I have found that having an identification card in your alternative name to be very helpful. 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 alternative 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?”

What phone number should you put on the back of the membership card? I will present some ideas in a later chapter.

Events

Many events, concerts, and various forms of entertainment now require a credit card for attendance. Most events allow the purchase of tickets through a single vendor. The tickets must be purchased either online or via telephone and mailed or picked up at the ticket area of the event. When you purchase tickets, you are usually required to give all of your personal information including full name, home address, home telephone number, and date of birth. With your secondary credit card, you should only provide the name on the card, and your post office box if the tickets will be mailed. There is no verification on any additional information. Ultimately, the company just wants to be paid for the tickets. Any other information they collect gets passed on to databases for the marketing division.

Utilities

In 2011, I assisted a colleague that was receiving very serious death threats to him and his family. It was serious enough that he moved his family to a new home that he purchased in a business name. He was having issues obtaining services to the residence without providing his complete personal information including a social security number for a credit check. He had reached a dead end with the cable company responsible for internet access in the area. They refused

to provide internet service to a business name in a residential area. With his permission, I contacted the cable company on his behalf and reached a fairly polite customer service representative. My friend had already obtained a secondary credit card in another name on his primary account.

I advised the representative that I wished to initiate new service at my residence. I provided the address and the name on his new card. When she asked for a social security number, I informed her that I had been advised to never give that out over the telephone and requested an alternative way to verify my identity. As expected, she stated that I could place the monthly charges onto a credit card and warned me that the charges for the entire month would be applied immediately. I agreed to that and provided the card number. This eliminated the need for them to conduct a credit check. They now had a credit card number on file for automatic billing for the upcoming month. If the charges failed to go through, they would be able to disconnect service.

This method will not always work. I have been declined by one representative only to be approved by another with an immediate second call. Persistence often pays off. Power providers and water companies are less likely to accept automatic credit card payments. Fortunately, they are usually willing to bill the customer in a business name. This will be further explained in the next chapter.

Legalities

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 that you have authority over. Additionally, you must always follow these rules:

- ✓ Never provide your alternative name to any law enforcement or government official.

- ✓ 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 that a credit card is needed.

Prepaid Credit Cards

If you are not ready to jump into using an alternative name, a prepaid credit card may be better for you. A prepaid credit card is not a true credit card. No credit is offered by the card issuer. Instead, the customer purchases the card by paying the entire balance of the card upfront. A prepaid card with a balance of $500 would cost the customer $500 plus a small fee. This card can now be used anywhere that traditional credit cards are accepted. When the balance of the card is spent, the card is no longer accepted. These cards can be purchased at many retail stores.

American Express

For the best economic value, I recommend the American Express prepaid cards. They occasionally offer to waive the fee associated with the card and I stock up. Further, they offer a business gift card that you can customize. Navigate to their website at americanexpress.com/gift-cards and choose the “Custom” option. This will allow you to choose the quantity, dollar amount, and two lines of custom messages. These messages will appear directly below the credit card number where a person’s name usually appears. You can get as creative as you want, but remember that American Express will manually approve or decline each submission. I have found the following to pass any scrutiny.

Michael Smith (Any Name)
Travel Adventures LLC (Any Business)

Michael Smith (Any Name)
Business Travel Card (Any Purpose)

The Estate of Michael Smith (Any Entity)
Account # 85367 (Any Number)

Cards that possess some sort of customization often pass scrutiny more than those that do not. A benefit of this card is that your name is in no way associated with it. You can provide any name you want when making a purchase. When the company you are dealing with applies the name to the card for the purpose of charging the account, the prepaid card company disregards any name submitted. The card company knows that this is a prepaid card and allows any name to be used. In this example, American Express will need a real name and credit card to complete this transaction and send a gift card. This may be invasive for many readers. The next technique should solve this issue.

Vanilla Visa/MasterCard

For the most private prepaid card, I recommend the Vanilla Visa and MasterCard options. These do not require any personal information and can be purchased at numerous stores with cash. After purchasing the card, it is ready to go for any in-person purchases. If you want to use it for online purchases, you only need to register it through the Vanilla website. This registration will ask you for your postal code. You can provide any code that you want, but it should match the code that you will be providing on any orders. I have had numerous experiences with these cards and have found the following to be helpful.

- ✓ You can change your postal code at any time on the Vanilla website. You may change this as you make online purchases using different physical addresses.

- ✓ You can purchase card increments up to $500. I suggest purchasing larger denominations to avoid numerous cards with small leftover

balances.

- ✓ You can purchase cards in Canada while using them in the United States. You will pay a small conversion fee, but the extra layer of privacy is nice in some cases. You can change your postal code from a Canadian code to U.S. code at any time. I use this technique when purchasing online services such as VPN's.

- ✓ Any name and physical address entered during an online order will be accepted.

I often use prepaid cards when traveling. If one gets lost or stolen, I do not need to worry about unauthorized access to my true credit accounts. If the card information gets "skimmed" by a dishonest employee of a business I visit, the damage will be minimal. Any purchases I make will be completely anonymous and I will not be subject to future marketing attempts.

I recently had a client that wanted to purchase a completely anonymous VPN service and Blur account. He wanted to use an alias and have no connection from him to these services. After establishing proof that he did not want to do this for malicious purposes, I offered to help. While on a business trip to Toronto, I stopped at a grocery store and purchased a Vanilla Visa with Canadian cash. I activated this card while connected to a local hotel Wi-Fi and supplied the postal code of that hotel. I used the card to purchase the VPN services and Blur subscription while on this network. I provided the credentials to the relieved client. This may be overkill to most readers. However, to someone in fear of his life, the scrutiny to both privacy and security is justified.

Virtual Credit Cards

When you make purchases online, you are at risk of your credit card getting compromised during a database breach. These thefts are so common that they rarely make the news. A criminal can obtain thousands of card numbers at one time by breaking into a business's servers. If your number is in the database, you will probably be a victim within hours. To avoid this, you can use virtual credit cards.

A virtual credit card, sometimes referred to as a temporary credit card or throw away credit card, is a credit card number that is generated by your credit card issuer on your behalf for temporary use. You don't actually get a physical credit card with this number. You simply use the number for an online transaction and then it expires.

Any time that I need to order something on the internet from a questionable source, I use this option. Some people have been known to provide these numbers for free trials that require a credit card. If the company tries to apply an unauthorized charge, it will be declined. Citi and Bank of America offer this free virtual number service. You should contact your credit card company to find out the options available to you. If it is not, I highly recommend the service Blur.

Blur (abine.com)

Blur was mentioned earlier in the preparation chapter. It is a premium service that provides masked email addresses, telephone numbers, and credit card numbers. As stated earlier, it is one of my favorite new privacy enhancing services. If you are serious about privacy, and desire the conveniences of credit card transactions, a Blur account is vital.

Blur's masked credit cards work the same way that a banks' virtual cards function. It is very similar to a prepaid credit card. When you wish to make a purchase online, you log into Blur and create a new masked card. Blur will generate a unique credit card number complete with expiration date and CCV. You can use any name you like with the card and use Blur's Boston address as the billing address. Be aware that to use a Blur card you must know the total purchase price, including taxes and shipping, and create a card for at least that amount. However, unused balances can be refunded.

This allows you to make purchases online without giving out your real credit card number that could be stolen in transit, leaked in a data breach, or otherwise compromised. It also limits the amount of information your credit card company has about your shopping habits and helps to prevent merchants from building accurate data profiles about you. I use this service every time I make a purchase online. The following details outline a typical use scenario. Assume that your goal was to purchase a VPN service for $69.95, pseudo-anonymously, but use

your real credit card.

- ✓ Create a premium Blur account and pay for the service with a Vanilla prepaid credit card. Do not add this prepaid card as a credit card into your Blur Wallet. This is only for the payment for the service. Use your secondary credit card alias as your name for the account and provide a non-existent physical address. The prepaid card will successfully charge with any billing address. The reason you should consider making the initial payment to Blur using a prepaid card rather than your secondary card is that Blur will always keep a record of your initial purchase. However, any cards that you add for payment purchases once you have Blur can be removed and these records will be purged.

- ✓ Provide a 33 Mail email address to Blur for contact and login credentialing.

- ✓ Add your secondary credit card to the Blur wallet. This will be your actual credit card number as assigned to your secondary alias name. This will be used by Blur to charge any purchases for masked credit cards.

- ✓ Log into Blur and create a new masked card. Give the card a descriptive name you will remember and choose an amount of $69.95. Blur will display your new prepaid credit card number, expiration, and verification code. Your real credit card will be charged exactly $69.95 plus a $2.00 fee from Blur.

- ✓ Purchase the VPN, or any other goods or services, with this new prepaid credit card number. If required, provide Blur's Boston physical address which will be visible on the new masked card in your account. You can provide any name to the provider, as any option will successfully charge to the Blur number.

You now have the new service that you desire, and the provider of the service knows nothing about you. The masked credit card number used is now invalid,

and your real credit card was charged $69.95 by Blur. Your credit card provider does not know what you purchased. The VPN service provider believes you live in Boston and does not know your name. If the service tries to charge a renewal fee to that credit card number, it would be declined. You will not have any surprises and do not need to worry about cancellation to avoid recurring fees. There are two basic strategies to use with Blur; single and continuous.

Single: Each time you need to make a purchase online, create a Blur masked card for the exact purchase amount. The card will expire immediately after use. The benefits here are unique numbers for every purchase and the inability for any unauthorized purchases. The negative aspect is the need to access your Blur account and create a new card each time you wish to make a new purchase.

Continuous: Create a Blur masked card in a generic amount such as $200. Use this number as you would a prepaid card and make small purchases until it is depleted. If there are a few dollars remaining on the masked card, simply refund it back to your credit card through Blur. The benefit with this method is that you always have a prepaid credit card number available for immediate online purchases. The concern is the ability for unauthorized charges and an association of all purchases through the single credit card number.

Occasionally, an online merchant will want to verify that the credit card being used was not stolen. They may want the complete billing address associated with the account or the issuing bank's address and telephone number. If this happens, Blur allows you to provide their verification information. The billing name and address associated with all masked cards is Abine, Inc, 280 Summer Street, Boston, MA 02210. The telephone number associated with that billing address is 617-345-0024. The bank issuer of the cards is Wex Bank.

Prior to August 14, 2015, I applied both methods to my privacy strategies. I would create unique numbers for every online purchase when possible. The masked card was in the exact amount of purchase. I also maintained a handful of prepaid Blur numbers that carried a balance for immediate availability while travelling. However, Blur's policies changed on that date. As of this writing, Blur charges $2.00 per masked number for cards with a value up to $100.00. An additional 1.5% is charged to cards with a value above $100.00. Blur also charges $5.95 monthly to any open cards with a balance after 30 days.

Therefore, I have adjusted my strategy for Blur masked cards.

Blur currently allows you to connect a banking account to your Blur account. This allows for masked cards at no cost. Due to the lack of fraud protection normally provided by debit card companies, I have not tested this.

When I need to make a purchase, I continue to create a new masked number in the exact amount of the purchase price. If I expect to make any additional purchases within the next 30 days, I make the total value of the masked card $100.00. That will leave a balance to the card without any additional fees. If I do not deplete the balance within 30 days after the creation, I refund the remaining balance to my secondary credit card on file. With this method, the total expense for the service is $2.00.

I have seen some minor issues with Blur. A client recently made a purchase through a smaller online merchant using a Blur credit card number and billing address. However, he was shipping the item to an alias name at a friend's house. After thirty days, the package had not arrived even though the merchant had sent a shipping confirmation email. Upon contacting the merchant, my client learned that as a matter of policy the company only ships to the billing addresses to "prevent fraud". The client contacted Blur who explained the issue to the merchant. The company sent a new item to the shipping address. Situations like this are very rare in my experience. However, if you purchase through a small operation, you may want to contact them before completing your purchase to ensure that they will ship to an address other than the billing address.

At the time of this writing, a premium Blur membership costs $39.99 per year, $59.99 for two years, and $79.99 for three years. Blur occasionally offers lifetime memberships at a reduced rate. I encourage you to contact them and ask about upcoming promotions. According to Blur, the surcharges on masked cards are actual expenses passed down from the credit card companies. In most uses, this will still be more affordable than the standard $5.95 fee that is associated with most physical prepaid cards.

Utilities and Residential Services

As a reminder, you can have all of your bills delivered to your post office box. I recommend contacting each credit and utility company that you have service with and request a mailing address change. The service will still be provided to your home, but the database of customers will list your address as your post office box. If this database is sold, traded, or compromised, the information will not identify your home address and landline telephone number. This can help keep you off marketing lists. It will also hide your residence from public view of data mining company reports. Later chapters will provide more ideas for your own custom strategy.

Summary

I believe that applying the methods discussed in this chapter is vital in order to achieve privacy in your daily life. Every reader of this book should consider a credit freeze. There are no longer any valid reasons for putting this off. Also, please consider obtaining some Vanilla Visa prepaid cards. These can be used in person anywhere that credit cards are accepted, but not always over the internet. I rely on my secondary credit card in my alias name almost every day. Again, I have found Chase to work best for this.

Proactively setting up your secure and private credit strategy is always better than reacting to the next breach. Having your system in place will bring comfort the next time that you are advised of another hacked database. During the writing of this third edition, I was notified by three companies that I was the "victim" of a data breach. The following will explain each scenario.

- ✓ I was notified by a hotel that I frequent that they had discovered malware on their point of sale systems. Hackers likely obtained my name, email address, credit card number, home address, and telephone number. I used an alias name, my secondary credit card, and a fake home address. If I see unauthorized purchases on my card, I will cancel it. No other information was real.

- ✓ I was notified by an online business that hackers had breached their customer database. They likely obtained my name, address, telephone number, email address, credit card information, IP address, and purchase history. I had used a fake name, my orders were

shipped to a PO Box, and I paid with masked Blur credit card numbers. My email and telephone number were forwarding accounts. The data collected on me is useless.

- ✓ I was notified by a newspaper that I receive that their customer database was compromised. The data stolen likely included my name, home address, payment details, and telephone number. I used an alias, paid with a prepaid credit card, and provided a Google Voice number. While my real address is known, there is no data associating it with my real name.

In all of these situations, I have no concerns. By creating my credit strategy, I no longer allow companies to store real information about me. I can no longer trust the security of these institutions. If criminals attempt to use the data in my record to steal my identity, they will fail every time. This is great peace of mind.

Chapter Six

Anonymous Purchases

The previous chapter explained the importance of a credit card in an alternate name. I rely on this technique during much of my travels. However, this is no longer reserved only for traveling. On a daily basis, we all make purchases that require credit cards or personal information. The days of living solely on cash are almost gone. While it is still possible, and many people do it, it has become increasingly difficult. Many toll roads no longer accept cash. If you do not have a digital pass attached to your front windshield, you will be billed at the address attached to your vehicle registration. Most airlines will no longer accept cash for in-flight purchases. You must have a credit card.

This chapter will explain various ways to protect your privacy while maintaining the convenience of making non-cash purchases online and in person. Before outlining these techniques, I feel obligated to examine how convenience is inversely proportional to privacy and security. The more convenient something is, the more personal privacy and control of your identity you are probably sacrificing. Credit and debit cards are one such convenience. With cash you have to make time to visit an ATM, carry bills, and manage change. All of these inconvenience factors are compounded if you make multiple small purchases throughout the month.

Despite its inconveniences, making these multiple small purchases routinely is precisely the reason you should use cash when available. Though it is certainly more convenient to swipe a credit card for purchases than it is to use cash, it also creates a tangible, searchable record of each transaction. Your purchases record a wealth of data about you including your location and movement, interests, hobbies, and a plethora of other information. Some will say that this data is protected and only visible to those with proper authority. I counter that argument

with whatever data breach is in the headlines while you read this chapter. Further, history has proven that those with proper authority sometimes abuse their power.

A client of mine did not fully realize the extent to which his personal pattern of life was spelled out in black in white until he bought his first home. One of the requirements for the loan application was to submit three months of statements for all bank and credit accounts. He was very disheartened when he had to submit statements for several accounts that looked something like the following.

Date	**Transaction Description**	**Amount**
07/01/15	Debit – Local Grocery Store #1	$17.35
07/01/15	Debit – Local Grocery Store#2	$31.53
07/02/15	Debit – National Coffee Chain near Work	$4.88
07/02/15	Debit – Convenience Store near Work	$2.37
07/02/15	Debit – Lunch Restaurant near Work	$12.72
07/02/15	Debit – Gas Station	$43.68
07/02/15	Debit – Local Grocery Store #2	$8.19
07/03/15	ATM Withdrawal	$60.00
07/04/15	Debit – National Coffee Chain near Work	$4.88
07/04/15	Debit – Big-Box Department Store	$81.41
07/04/15	Debit – Local Dinner Place near Home	$27.12
07/04/15	Debit – Large National Bookstore	$27.19
07/05/15	Debit – Fast Food Place near Work	$6.01

Years prior, he had subscribed to the philosophy that plastic is easier to use, and somehow inherently better, than paper. What he did not realize was that he was sharing a ton of personal details about his life with others. With the information above, which only covers a period of five days, he reveals where he shops for groceries, where he gets coffee and eats, and where he gets fuel. If this information is multiplied by six to accommodate the entire month, even more information is revealed. Details such as the frequency of eating out, getting coffee, or visiting the bookstore are revealed. If this information is coupled with the retailers' records, I could know exactly what he buys and how often. Within a few months, I could begin to predict not only where he shops, but what he buys and the meals that he consistently orders. Though there was nothing "shady" on his cards, it was more than a little embarrassing to share such granular level of

detail about his life with strangers.

He realized that he had been sharing all of this information with his bank and creditors for several years. Additionally, many stores where he shopped kept a detailed record of the items he purchased based on his credit card number. Some stores even tout this as a convenience measure, allowing you to get a refund without receipt based on your credit card. In reality, this information helps them send targeted advertising to you. Have you ever used the self-checkout at the grocery store and received coupons printed immediately after purchase? If you look closely at the items that are promoted in these coupons you will probably notice that these are based on your credit card's shopping history.

Purchasing with cash offers much more anonymity. Unless you are purchasing something that requires you provide your real name, purchases with cash are about as close to anonymous as you can get. The purchase of firearms and cars are obvious exceptions that will be discussed later. With most cash purchases, there is no paper trail, no bank statement, and no record of your life and activities. If he had it to do over again, he would have made some changes in his personal habits. His account statements would have reflected the same period of time a bit more succinctly similar to the following.

Date	Transaction Description	Amount
07/01/15	ATM Withdrawal	$500.00
07/08/15	ATM Withdrawal	$500.00
07/20/15	ATM Withdrawal	$500.00

You will notice that if he had used cash, this brief statement covers a period over four times as long as the above example, while still being eight lines shorter. Not only is this statement more compact, it also reveals very little about him. It does not reveal where he buys his groceries or the location his favorite coffee, lunch, and dinner restaurants. You cannot see his culinary preferences. It does not associate his name to any of his purchases.

I attempt to use cash as much as possible but realize that I will never be able to fully eliminate credit cards from my life. Air travel, rental cars, and hotels require credit cards. I still find myself in locations where I don't want to pay exorbitant ATM fees, and end up using a credit card. But I use it a lot less, which

is what I am truly advocating. Use more cash and less plastic. This reduces the amount of information about yourself that you give over to your bank, your lenders, or anyone curious enough to swipe a statement out of your mailbox.

There are significant and compelling reasons to keep your purchase history anonymous. Your purchases reveal almost everything about you. The sporting goods you buy (or don't buy) probably say a lot about your level of physical activity and fitness. The books you read reveal a lot about your personality including your religious beliefs, your political leanings, your sexuality, and the things you are passionate about. The foods you buy, the restaurants at which you eat, the frequency at which you eat at them, and the alcohol and tobacco products you consume reveal a lot about your health. This may one day very soon be used to calculate your health and life insurance premiums.

Using cash isn't bulletproof, and it won't make you totally anonymous. It will lower your digital signature, offer you a lot more anonymity, and make an attacker's job a bit harder. Every bit helps. For those situations that do not allow cash purchases, I have some ideas that will decrease the invasive tracking of your buying habits.

Online Purchases

Do you remember a day when you would go to the grocery store for all of your food, the hardware store for replacement parts, and the department store for household goods? For many people, this has all been replaced by online retailers such as Amazon and Ebay. Even specialty crafts and artwork is now sought through websites such as Etsy. You can avoid these types of companies and still get what you need with cash at physical stores. However, you will miss out on the convenience and affordability of online shopping. This section will guide you on maintaining your privacy while using these services.

Amazon

I begin with Amazon because it is one of the largest online retailers. 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. The details that you provide are very important. Before discussing the appropriate methods, please consider an actual scenario.

A client had recently 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. The following steps will mask your real identity from your Amazon purchases. This technique can also apply to other online retailers. Create a new account with the following information.

- ✓ **Name**: Use the name that you want your packages shipped to. This could be the former resident or landlord at your address, or a complete alias.

- ✓ **Email Address**: You must provide an email address for your new Amazon account. I recommend using a forwarding email service

such as 33mail.com as discussed earlier. If your 33 Mail user name is "privacy", you can use an address of amazon@privacy.33mail.com. This new Amazon account will never be associated with your real name, and it will not be connected with any of your real email accounts.

- ✓ **Credit Card**: If you have a Blur account, create a new masked card and title it Amazon. Add a balance to it with at least $100. Supply this masked card number to Amazon and provide the alias name that you want to use for deliveries. Use the Boston address provided by Blur for the billing address. If you do not have a Blur account, you could use your alternate credit card number, expiration, and security code. This number will be the same number on your real credit card, so be sure that this number is not in use on any existing Amazon profiles. Blur is recommended.

- ✓ **Address**: If using Blur, provide your shipping address as desired. This may be your actual home if you do not have a better place for deliveries. If you do not have a Blur account, provide the PO Box that you used for your credit card billing address. You can alter this information after the account has been verified. In the settings of the account, you can add a new address for shipments. I have used my real home addresses in the past for deliveries. Because the name on the shipment is not a real name, I do not see this as a privacy concern. I believe it helps establish that someone else lives at your residence, and provides great disinformation. You should scrutinize any option that you choose and make sure that it is appropriate for your scenario.

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. However, I encourage you to take things a step further and apply a bit more paranoia to your plan. I create a new Amazon account after each Blur card has been depleted. If I add a $200 Blur masked card to my account, and then use those funds over a period of five orders, I do not add a new masked card to my Amazon account. Instead, I close the account and create a new one. If there is a small amount of money remaining

on the Amazon masked card, I refund it through Blur back to a credit card. This way, Amazon does not have a single record of all transactions. Additionally, each Amazon account is in a new alias name for both shipping and billing. It will add disinformation to your address and will confuse your delivery person. The only drawback to this is if you subscribe to their Prime membership. You may want to create one account to be used with those benefits, such as free streaming movies.

Amazon Gift Cards

An alternative strategy for purchasing anonymously on Amazon is to use their gift cards. These are available for sale at many retailers including drug stores such as CVS and Walgreens, grocery stores, and even hardware stores such as Home Depot and Lowes. They can be purchased in amounts up to $2,000.00, require no additional activation fee as prepaid credit cards do, and some retailers require that you pay cash for them. Using these cards is incredibly simple. Create a new Amazon account, navigate to your payment settings, and add the gift card. When you have used up your gift card balance of $25, $50, or even $500, open a new Amazon account providing your real shipping address and a false name. Now order items from Amazon as you normally would. This creates disinformation rapidly. Within 30 days of making a purchase on an alias account, you might begin receiving junk mail at your home address in that name.

One minor disadvantage to this strategy is that you may end up abandoning a small balance of a few dollars on each account. This can add up to a substantial amount over time. I attempt to mitigate this as much as possible by carefully calculating my last few purchases to use the maximum amount of the balance possible. If there is under $5.00 left on the account, it can typically be used to purchase a movie or Kindle book (see the next section). Taken to the extreme, you could use this technique to make a new Amazon account, complete with a new name at your shipping address for every purchase you make.

Kindle and Other E-book Readers

You may be reading this book right now in digital form. If so, your reading device is likely sharing a lot about you to the service that supplies your books. If you are using a Kindle, Amazon stores the following about you in your profile:

- ✓ Books that you have purchased
- ✓ Books that you have read
- ✓ Books that you have searched from the device
- ✓ The last page read of any book in your account
- ✓ Any annotations, highlights, or markings within the book
- ✓ Speed at which you read any book

Some will argue that this is not a big deal. Those people probably did not make it this far into this 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, they 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 brewing beer, 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 brewing beer at home may be painted to make you look like an alcoholic.

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 the connection off. 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 Blur credit card for added privacy. Never attach this account to your real name or address. Ship the device to your PO Box. Register the device with this account and use any alias name for the Kindle.

- ✓ Turn the device on while outside of 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 that purchased 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. Further, 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.

EBay & PayPal

EBay and PayPal, which are owned by the same company, can be trickier. EBay

will apply some minor validation to the data that you enter and will require a valid form of payment to make a purchase, such as your alternative name credit card. PayPal will also require this valid form of payment and will request a social security number that will only be used for income reporting. I have had mixed success with using alias names. The following information may be useful.

- ✓ EBay will accept an alias in order to create an account. You can also use a 33 Mail email address. You do not need to use your real name.

- ✓ EBay will accept masked credit card numbers generated from Blur. The billing address must be Blur's address in Boston. Any other address will fail verification.

- ✓ PayPal will allow you to create an account using an alias name and address. The address must actually exist, and library addresses do not appear to be blocked. They appear to accept 33 Mail email addresses, but not NotSharingMy.info accounts.

- ✓ PayPal will accept Blur masked numbers if you provide your home address as the Boston address for Blur. They will not accept all prepaid cards. The address on file at PayPal must match the address on file for the prepaid card. I have found the Vanilla prepaid card to work on one occasion but not a second. This will be trial and error.

- ✓ PayPal will not accept "Load Money" PayPal gift cards if you have not verified your identity and provided true financial information. Avoid purchasing these as you will not be able to use them anonymously.

- ✓ If you want to sell items on EBay and/or accept payments through PayPal, you will need to provide a valid social security number and banking information. I believe you would be better suited using Craigslist and accepting cash only.

Everything Else

For the most part, any online retailers simply want to be paid. If the credit card that you use is valid and matches the shipping name and address of the purchase, the order should go through. There is not much other validation when you complete the sale. There is no reason that you should not be able to use your alternate name credit card for all of your purchases. Eventually, your UPS, FedEx, or USPS delivery person will start to believe that you are named the alternate name on your card. Some have called me this name during deliveries.

Store Purchases

In 2012, I purchased a new refrigerator. The large home improvement store that had the best price won my business. They also offered free delivery to my home. I sat down to complete the purchase with the salesperson when the questions began. In order to sell and deliver a refrigerator, I had to provide my name, home address, telephone number, cellular telephone number, work telephone number, credit card information, and a secondary contact person. Obviously, my address was necessary, but I am hesitant to provide the rest. Later in the book, you will read about the ways that data marketing companies learn information about you and resell the data. This is one of the primary ways that you are targeted for future purchases. As soon as you provide this information, it is added to an internal database and resold to other companies. The following is how I handled the situation.

- ✓ **Name**: I advised that this purchase was for my father, so I would like the delivery in his name. I then provided a very specific name such as John Coolman. Why Coolman? The last name Coolman will remind me of my “cool” refrigerator. I choose a name like that because I want to monitor where the data provided to the salesperson is sent. In a few weeks, when I receive a mailing from an advertiser to John Coolman, I will know where that company received the information.

- ✓ **Address**: I provided my home address for the delivery. Because this was not associated with my real name, and I needed to tell them where to go, this was acceptable.

- ✓ **Telephone Numbers**: I advised that there is no telephone at the house but I will be available on my cellular number at any time. I then

provided my Google Voice account.

- ✓ **Payment**: I used my alternate name credit card.

- ✓ **Secondary contact and work number**: I assured the salesperson that I would be available and a secondary contact or work number was not necessary.

This may all seem very basic and like common sense, but think about what took place. I kept the purchase anonymous with my alternative name credit card. I added another layer of privacy by placing the delivery in a generic name. That generic name will never be used by me again and will help me identify where that store shares my information. I will not personally be targeted with offers of extended warranty protection. My real name will not be added to the database of large product purchases that will receive future promotional offers. Finally, I have a receipt that will suffice for any issues with the product.

Any time that I make a purchase that requires delivery; I never use my real name. Doing so would add my name and address to various online websites from which I have previously removed them. The additional benefit is that this disinformation that I provided will now be associated with my home address. It will confuse data marketing companies about the actual tenants. The next chapter will expand on this concept.

Remember, we are keeping everything legal because we are not causing any financial fraud. All of my purchases are billed to a credit card number that is assigned to us. We will pay the bills as agreed with my credit card company. These transactions will not financially affect anyone else.

Many purchases will ask that you to fill out a warranty card. I have purchased items as large as refrigerators and as small as coffee pots that include a "Warranty Registration Card" in the package. I strongly advise against filling these out with accurate information. Your receipt is a legally-accepted proof of purchase for the item. The warranty registration card is merely an attempt to lure you into providing personal information that can be sold. Warranty cards also offer an excellent opportunity to create disinformation which will be covered in

a later chapter.

One big lesson in regards to in-person purchases is that you always have a name, address, and telephone number memorized at checkout. If paying by secondary credit card in an alias name, you should use that name if asked. However, the physical address and telephone number provided during an in-store purchase is not verified with the credit card being used. This is collected for that store's internal marketing database and will likely leak out to third parties. Take a moment now and start thinking about the address and telephone number that you would give out if asked.

Many businesses will demand this information from you as a customer. In a blog post, JJ Luna shared his experience with purchasing a new pair of glasses at an optometrist. He was paying cash, but they insisted on collecting his home address and telephone number. He argued that the cash sale did not require that information, and they refused to serve him. He walked out without the glasses. While I certainly respect his response, there may be situations that you face that will not allow you to simply walk away. Instead, always have an address and telephone number ready. A later chapter will present many examples of safe information that you can use to protect your privacy while functioning in today's society.

Online Payment Methods

The world has changed drastically when it comes to cash purchases. Prior cash transactions for Girl Scout cookies in front of a grocery store have turned into credit card processing by children. Several new services have made it incredibly easy to accept credit cards for payment at any time. PayPal, Square, and others have introduced free credit card readers that attach to any smart phone. They then use the phone's internet connection to process the payment through secure servers. While this has not helped the fight to preserve the anonymous option of cash, we can still use it to our advantage.

If you want to make a purchase from someone that accepts these forms of payment, you are not required to use an actual credit card. The focus of these readers is the ability to swipe a card for payment. However, the owner can also accept a virtual credit card as payment. Consider the following two scenarios.

You are at a mechanic, art festival, or used musical instrument shop and you want to make a purchase. The items that you want to buy exceed the amount of cash that you possess. The seller has a Square credit card reader connected to his iPad and can accept credit card payments. Advise him that you want to use a gift card that you received via email. The seller can type the credit card number, expiration, and security code into the Square app on the device to accept the payment. A physical card is not required. When you give him a masked credit card number issued by Blur, you can associate any name with the purchase. If the purchase is a high dollar amount, you may be required to present the billing address of the card. When using Blur, you would give the company address of 280 Summer Street in Boston. I have used this address so often that I likely receive postal mail there.

You have identified an item that you want to buy on Craigslist. The seller will accept PayPal as a form of payment and can either swipe a credit card through the PayPal reader of accept a transfer of funds from your account. Instead, ask the seller to issue you an invoice from within the PayPal account. Give an email address connected to your 33 Mail account. You will immediately receive an invoice via email from PayPal for the exact amount. Use a masked credit card from Blur to complete the transaction without creating a PayPal account. When prompted, simply choose to pay by credit card.

I believe that our society is going to see more adoption of electronic payment and fewer opportunities to buy with cash. While disappointing, we must go with the flow. Knowing your options ahead of the transaction will prepare you to stay as private as you can. Being prepared with an alias and virtual credit card will take you a long way.

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 on 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 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 that 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 they could reach her at during delivery. She panicked and hung up without giving them any details. She then called me.

If she had completed the order, there would be a very strong trail from her current 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 that 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 that allow you to store your belonging in 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.

The 33 Mail email address on file received a confirmation that the containers had arrived in St. Louis six days later. 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 new city that she was moving to. 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 that I was moving to. I then gave this company her actual address 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.

At the end of this move, I paid for the following services using the client's secondary credit card.

- ✓ U-Box drop-off at original location
- ✓ U-Box pickup at original location
- ✓ U-Box storage for one month
- ✓ U-Box delivery from Miami to St. Louis
- ✓ Independent moving company delivery to new residence

- ✓ Independent moving company empty container return fee

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 where she moved from. 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 where she came from. 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.

Her first purchase at the new apartment was DirectTV satellite television service. She placed the call for the order through a Google Voice number and provided an alias name with her real address. She asked for paperless billing and requested her credit card be automatically charged prior to each month of service. She again provided the secondary credit card in her alias name. Because she was enrolled in automatic billing to a valid credit card, there was no approval process or credit check. Most services will bypass this requirement by enrolling in a type of auto-pay option.

Internet Service

I believe that the most import utility or service that you can anonymize is your home internet connection. Possessing internet service at your home address in your real name jeopardizes your privacy on two 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 that you are connecting to their system.

Those that use other technologies 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 that 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 that 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 law suit 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 that 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 that are seen as infringing? I believe a 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 explained later. 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 recent 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 did 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 for this book.

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 obtain 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 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 negotiate that cost down through threats of cancelling when the time came.

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 credit card. I was told that I could set up the automatic payment ourselves after the account had been established. This was even better. 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 second to evaluate the risk and provided a year of birth that 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 literally 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. He then activated automatic payments to that card and enabled the paperless billing option. Today, he continues to receive

great internet service from Charter and pays his bills automatically to his secondary 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 was 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 a SSN. The first employee stated that a 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 a 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 were told that the deposit would eliminate the requirement. I have had two clients since these conversations that have confirmed that Comcast will provide service to any name provided 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 hard credit check. This will associate your real name with the address of service (your home).

DOB/DL Required: If the provider requires a date of birth or driver's license number, this is also a strong indication that a 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 announce your name to your address and will be present through online resources.

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

Your experiences may vary from mine. Overall, most internet service providers stated that a 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 was recently the victim of identity theft and was told to no longer disclose my SSN. Is there any way I can purchase your services without giving you my personal details? I will pay the deposit.

- ✓ I reviewed your website offer details and I want to purchase internet service though your company. I will be paying automatically by credit card in order to forego giving you my SSN or DOB. Thanks!

I encourage you to be persistent and do not give into the sales tactics. Overall, the person you talk to wants to complete the sale. Hopefully, this chart will help you choose an internet provider that values your privacy. Later in this book, I will discuss strategies for making all of your utilities anonymous.

Incoming Mail

Your purchases prior to reading this book are likely to have an impact on the mail that you receive today. After you complete the data removal process in this book, pay close attention to the mail that you receive at your home. Each piece

should be categorized as either junk or important. If it is junk, eliminate the mailings through Catalog Choice or DMA. If the mailing is something important that you want to continue to receive, contact the sender and change your address to your post office box. If you have an online account for the company, attempt to change this yourself through their website. Any mail that you send out should always have your post office box address instead of your home address.

If you receive advertisement in the mail addressed to your name at your home address, you may want to contact the sender and asked to be removed from the mailing list. In my experience, this seldom works. Reputable companies may honor your request. However, many companies simply ignore it. When you believe this happens, I recommend calling and changing your address. Consider the following actual scenario.

I had a client that had a taste for expensive vehicles. He had purchased a few over the years, and he was now targeted heavily by a large local dealer. He had eliminated most of the mail to his name at his home address, but this dealer sent him a flyer, letter, or invitation every week. He called and politely asked to be removed from the database. This never worked. Finally, he called and stated the following.

“Hi, I have been shopping for a car at your dealership, and I have received some great offers. I just moved and I want to make sure I don’t miss the next big sale. Can you update my address?”

The dealership happily updated his file to include the new address that he provided. The address that he provided was that of a competing dealership located one town over. The receptionist that answered the phone had no clue.

Package Deliveries

Internet shopping offers cheap prices and global access to products. You have probably ordered a product from an internet company such as Amazon or Netflix. When you supply your home address for these deliveries, the information will be added to marketing databases. These databases will probably only be used for internal marketing from one company, but the data may

eventually be sold to other collectors. The best solution is to provide your post office box address for deliveries. Further, be sure to remove your residence address from your profile through the online retailer. If you have a mailbox that is not large enough for the delivery, you will receive a notification of a package available for pickup at the counter.

Another option is to have packages delivered to your workplace. This may not be appropriate for everyone. If you are a victim of domestic violence and you do not want anyone to know where you work, you should not choose this option. If you are a government employee, public official, or have a job with any public presence, there is probably no harm in using a work address. I choose to have everything delivered to my workplace. A package left inside a workspace is more secure than one left outside an empty home. Additionally, there will likely be someone available to sign for a package during business hours.

Food Deliveries

Ordering pizza or Chinese food does not necessarily compromise your privacy. You must disclose your address for the delivery, but you do not need to provide your real name. If you want to keep your home address private and unassociated with your name, always obey the following rules:

- ✓ Never provide your real name or telephone number.
- ✓ Never call from your landline telephone. It will identify your name.
- ✓ Never rely on caller ID to protect your information.
- ✓ Order online through the company’s website when available.
- ✓ Always pay with cash.

Chapter Seven

Anonymous Telephones

Cellular telephones are digital trackers in our pockets monitoring and recording every move we make. They are beacons announcing our locations, conversations, contacts, and activities to companies outside of our control. Do I use cell phones? Absolutely. Can I reclaim my privacy without ditching the convenience of a computer in our pocket? Yes, and I will explain my methods in this chapter.

I believe that having an anonymous cellular telephone is very high on the list of vital steps to take in order to obtain true privacy. Your device is always tracking you. If the device is on and connected to either a cellular tower or Wi-Fi connection, it is collecting and sharing your location information. The moment you place a call or send a text, you have updated a permanent database of these details attached to your account. Some will argue that these details are not publicly visible and only obtainable with a court order. While in a perfect world this is true, we do not live in a perfect world. There are many scenarios that could leak your entire communications history to the world.

The most common scenario would be a data breach. I hear every day that a new database of customer information has been stolen and released to the wild. What is to prevent that from happening to a cellular provider? I also know from widely publicized reports that some government agencies overstep the scope of data collection from both Americans and non-Americans, often including telephone records. I have seen several civil legal battles incorporate cellular records into the case after submitting a subpoena to a provider. I have even heard of rare instances where a Freedom of Information Act (FOIA) request was submitted for cellular records of government employees.

Regardless of your situation, I believe that you have a great deal of data to lose by using a standard cellular telephone setup. This chapter will explain many ways of maintaining privacy while remaining connected to the world. Near the end, I will share my current telephone strategy.

The most common way to possess a cellular telephone is through a contract with a major provider. This typically happens when you visit a provider's kiosk or store and are given a free phone. While this sounds like a great excuse to upgrade, you are committing to multiple years of service though this carrier. Privacy through this method is practically impossible since the provider will mandate a financial check on you using your social security number. Your phone, bill, and call details will be stored forever and connected to your name. Your cellular number will be associated with your name and available publicly online. This can all be avoided, but at a cost.

The rest of this chapter will assume that you are ready to change your cellular strategy. If you are currently stuck in a contract, you may want out of it. If you are no longer committed to the original contract terms, you are ready to ditch the service. Either way, it is time to break away from the comfortable options provided by the carriers.

First, I need to acknowledge that many readers are stuck in a contract and do not have the option of simply stopping the service. I understand that and want to help you eliminate that monthly bill. Every provider is different, but I believe it is always possible to force a company to release you from the contract. The following methods should be evaluated for your specific needs. Choose one that is most appropriate for your situation and attempt the technique. The worst that will happen is that you will be told "no".

Changes to Contract Terms

If your cell carrier changes the terms of the contract you signed, you can cancel your contract without paying any early termination fees. Many states require cell phone companies to give customers advance notice of contract changes which could increase the cost or extend the length of the contract. These cell phone companies must get consent from their customers before increasing the cost or extending the length of contract. Contact your provider and request a copy of the

contract that you originally signed. In a separate call, to a different representative, request the current contract terms for your plan. If the price, coverage, or usage limitations have changed, you can likely demand release from the contract. This method became very popular when Sprint changed their terms of service in 2008. Any customer that signed a contract before that date had the legal right to cancel the agreement without penalty. Providers are very aware of this trick, and will likely resist. However, persistence usually pays off. Third party services such as cellbreaker.com can assist with this technique. As always, if you create an account with CellBreaker you should use anonymous information.

Changes to Coverage

Most cell providers' coverage areas are quite extensive, but there will always be gaps in service. If you move to an area with little or no coverage, you may be able to get out of your contract. Keep in mind that most cellular service providers don't want to let you go, so they may offer you a mini antenna or tower for your home. This will often boost your signal enough to give you reasonable coverage. You can often use your provider's coverage maps to identify areas with weak reception. Stating that you have recently moved to an address within this non-existent coverage area will occasionally lead to termination without penalty. Currently, AT&T and T-Mobile have policies to release you from contract if you move to an area without service.

Document and Report Bad Service

I believe that anyone reading this section has suffered numerous dropped calls, awkward delays during a conversation, and the occasional absent signal. Complaining to the carrier and documenting these complaints can assist when you attempt to break your contract. You should always see if you can get your wireless provider to come around to your cause. They won't want to lose you as a customer, but most companies will make some kind of exemption if you talk to the right person and have a good reason. If you are a soldier who is being deployed, or you've lost your job and are unable to continue paying your contract, they'll usually let you out or work with you on a compromise.

However, don't expect to just call up and have the first person you speak to solve

your problem. You may need to call back several times or escalate your issue. Consider using the company's social media channels to your advantage, or go straight to the top and contact corporate executives.

Sell Your Plan

There is likely someone out there looking to get out of their plan and into a new one, and they may be interested in buying yours. You can choose to swap with them, or just sell your plan to them directly. Sites such as Cellswapper or Trade My Cellular attempt to make this painless. This doesn’t violate your terms of service because the other party is fulfilling the terms of your original contract. Again, if you sign up for such a service attempt do so as anonymously as possible.

Last Resort

There are also doubtlessly a few individuals reading this book who are nearing the end of their contract term, or who can wait a few months. Riding out the remainder of your contract is an option, as is paying an early termination fee. If you are only a few months away the early termination fee may be an affordable option for you. Regardless of how you do it, moving to an anonymous phone will not happen as long as you are on a contract. Getting off of a subsidized contract is essential, otherwise the steps in the remainder of this chapter will with useless.

I will now assume that you are free of any contract for cellular service and are ready to jump into a completely anonymous phone. Many people will mistakenly think that any pre-paid phone will protect you from intrusive provider practices. In reality, it is not that simple. Going to the local grocery store and purchasing a device with 100 minutes and 500MB of data using cash may feel private. However, there is much more to consider if you want to enjoy your new device and associated plan. The majority of pre-paid users possess inferior devices and over-pay for the limited service that they receive. I aim to correct all of that.

The Device

First, you will need a proper telephone. I never recommend any devices that are marketed toward pre-paid buyers. These are always the unpopular models that no one else wants. They are slow, have poor battery performance, and will only meet the minimum hardware requirements to function. Additionally, they are overpriced. At the time of this writing, a local grocery store was selling an Android smart phone for $149 that was available on eBay for less than $60. Either way, it was not a powerful device. Instead, consider a used phone.

Searching your local Craigslist.org community will identify hundreds of used devices for sale. You will need to be careful. Many of these are stolen, some are broken, and others are counterfeit. I recommend filtering these results until you are only left with the following.

- ✓ Devices that include the original box, cables, and manuals: This is an indication of a one owner phone that is not likely stolen property. A person that keeps those items probably takes good care of their property.

- ✓ Sellers that have recently upgraded: Many people must have the latest and greatest devices and upgrade the moment a new version is available. While you can never believe everything that you read on Craigslist, this is an indicator of a decent phone.

- ✓ High prices and old posts: Many people believe the value of their used equipment is higher than what others are willing to pay. Seeking phones that were posted over three weeks' prior at a high price will usually reveal people desperate to sell. Make a reasonable offer and you will be surprised how many people accept.

You may already have an unused device collecting dust. Usually, when you upgrade a phone, you are allowed to keep the old unit. You could use a device that was previously attached to your name and account, but I urge caution in this. Financially, it makes sense to use a device that you already have. Unfortunately, providers never truly forget what you have used. If you decide to use a phone that was previously attached to an account in your name, please know that the history will continue to be available.

Your device possesses an IMEI (International Mobile Station Equipment Identity) number that is transmitted to the carrier. When you activate an old phone, even as a prepaid, that number could still jeopardize your privacy. This may seem extreme, and it may not be important to most readers. If you want to completely start over and not contaminate your new communications device, you should obtain a unit that has no association to you.

If you are not concerned with the trail left to the cellular provider, then you can re-activate an old device. Only you can decide which is appropriate. I ask that you consider the following question. Will anyone ever ask your cellular carrier for a list of every phone that you have owned or used? By “everyone” I include hackers, friendly government agencies, enemy government agencies, the media, and general public after the next big data leak. In the most basic terms, your cellular telephone that was used in your real name is permanently attached to you. There is no way to break this connection. This device tracks your location at all times and reports to your provider. That data is stored forever. Therefore, I believe that now is the time to activate a new device with a new account.

I encourage privacy enthusiasts to start fresh with different new or previously-owned devices from strangers. You could also organize a swap with someone else that you have no official connection with. New non-subsidized phones are becoming more affordable while offering a level of privacy unavailable through a traditional contract. This might be a good time to try a different operating system. Android versus iPhone is a matter of personal preference. I have used both, and will outline my current devices, plans, and strategies for anonymity at the end of this chapter. You should use what you are most comfortable with. Both can be made secure and anonymous.

If you are looking for an extremely affordable solution, you might consider the various “Mini Card Cell Phones” available at online retailers such as Amazon. These miniature telephones usually cost $20 or less and are the size of a credit card. They do not contain touch screens, cannot use data plans, and do not work with apps. They can only make and receive calls and texts. I have used these as “burner” phones in hostile environments. The lack of data usage and internet access creates a fairly secure phone for minimal communication. These are almost always based on GSM networks and nano SIM cards.

Factory Restore

Regardless of the operating system, previous owner, or current state of the device, you should conduct a factory restore. This eliminates all personal data from any previous user and replaces the phone's operating system in the identical state as the day it was first purchased. This will ensure that there are no unique configurations that could jeopardize your privacy. The process for this will vary slightly by device. However, the following general practices should obtain the desired result.

- ✓ **Android**: Settings > Backup and Reset > Factory Data Reset > Reset Device
- ✓ **iPhone**: Settings > General > Reset > Erase All Content
- ✓ **Windows Phone**: Settings > About > Reset Your Phone

Rooting Android

Rooting is an optional process that gives you the power of full functionality of your Android device. It allows you to delete programs that could not be deleted normally and suspend processes that could normally not be accessed. I believe that this can be important for functionality, battery life, and privacy. However, this also makes the device much more vulnerable to malware and monitoring implants.

Each model of Android is unique and has a preferred method of rooting. Rooting will allow you to dive deeper into a phone's sub-system. Essentially, it will allow you to access the entire operating system and be able to customize just about anything on your Android. With root access, you can get around any restrictions that your manufacturer or carrier may have applied. You can run more apps, you can over-clock or under-clock your processor, and replace the firmware. The process requires users to back up current software and installing a new custom ROM (modified version of Android).

One of the most obvious incentives to root your Android device is to rid yourself of the bloatware that is otherwise impossible to uninstall. You will be able to set up wireless tethering, without paying extra, even if it has been disabled by your carrier. A lot of people are tempted by the ability to completely customize the look of their phones. You can also manually accept or deny individual app permissions.

There are essentially three potential cons to rooting your Android.

- ✓ Voiding your warranty: Some manufacturers or carriers will use rooting as an excuse to void your warranty. It's worth keeping in mind that you can always unroot. If you need to send the device back for repair, simply flash the original backup ROM you made and no one will ever know that it was rooted. In my scenario, the warranty has likely expired

- ✓ Bricking your phone: Whenever you tamper too much, you run at least a small risk of bricking your device. The obvious way to avoid it happening is to follow instructions carefully. Make sure that the guide you are following works for your device and that any custom ROM you flash is designed specifically for it. If you do your research and pay attention to feedback from others, bricking should never occur.

- ✓ Security risks: Rooting introduces some security risks. Because of this Google refuses to support the Google Wallet service for rooted devices. For my purposes, this will not be an issue.

Two recent rooting programs that have garnered some attention in the past year are Towelroot and Kingo Root. Both will root your device in a few minutes. However, both rooting programs are not compatible with every Android device. Searching these applications will present a list of compatible devices. If your phone is not compatible with the apps, you'll have to spend a little time researching ways to root on the Android forums. The best place to start is XDA Developers Forum. Look for a thread on your specific device and you are sure to find a method that has worked for other people. It's worth spending some time researching the right method for your device.

Cellular Service

After you have performed a factory reset and rooted your new device, you are ready to activate it on a cellular network. For complete privacy, I only recommend pre-paid plans. Subsidized contract plans require a real name or credit check but prepaid plans generally do not. Every major U.S. provider offers these types of plans. The following list compares the most affordable advertised services offered at the time of this writing. After, I will discuss a better option.

Service	Price	Minutes	Text	Data
AT&T:	$45	Unlimited	Unlimited	1.5GB
Sprint:	$35	Unlimited	Unlimited	1GB
T-Mobile:	$40	Unlimited	Unlimited	Unlimited*
Verizon:	$45	Unlimited	Unlimited	1GB

*Speed limitations on data

T-Mobile "Hidden" Plan

Privacy advocates have known about a hidden pre-paid plan at T-Mobile for a while. This plan, sometimes called the "Wal-Mart Plan", is not available at T-Mobile stores or kiosks. You will not find it advertised on billboards. In fact, it takes effort to locate the plan online. The plan gives you unlimited text and data, and 100 minutes of talk time, per month, for $30. The talk time may seem low, but that will not matter once you have your device properly configured for free unlimited calls. The following instructions will guide you through the process of obtaining a great anonymous phone plan at an unbelievably low cost.

- ✓ Ensure that you have a cellular telephone that is T-Mobile friendly. This device needs to support the GSM network. Most iPhone and Samsung Galaxy models will work. You should check the T-Mobile

website before you commit to this plan.

- ✓ Obtain a T-Mobile SIM card. Stores and kiosks will not offer you a card without committing to a plan. The T-Mobile website will send you a free card, but will require you to buy a more expensive plan. A third party online order is your best option. At the time of this writing, several vendors on Amazon were offering a T-Mobile SIM card starter pack, including a $30 credit, for $24.99 - $30.95. This is the best deal that I have found. Use the method explained in the previous chapter to create an anonymous Amazon account before ordering.

- ✓ Insert the SIM card in your device and turn on power. Have the SIM card serial number and the phone's IMEI ready. On a computer, navigate to the T-Mobile prepaid activation site and enter these details. On the next page enter your anonymous information. You can provide any name and address that you choose. This will not be verified. I recommend a common name and address that does not exist. Finally, it's time to choose the plan. Choose the $30 plan with unlimited text, data, and 100 minutes of talk time. Follow the activation prompts and you should possess an active phone.

- ✓ If you can make calls but cannot use data, manually enter the T-Mobile APN settings. Navigate to https://support.t-mobile.com/docs/DOC-2090 for specific instructions for your device.

You should now have a fully functioning, and fairly anonymous, cellular telephone. You should have fast 4G data, and the ability to install or uninstall any apps. However, this device is not ready for completely anonymous use. As mentioned previously, your phone is always tracking you, your calls and texts are being logged, and the data that you send is being monitored. You will need to make some modifications to the way that you use a cell phone. The following is an actual plan, from start to finish, that I executed for a client.

An Actual Sample Strategy

My client demanded an Android device. First, I purchased a used Samsung Galaxy S4 on Craigslist. It was listed at $125, and the ad had been posted over 30 days prior. I offered $75 and obtained the device at that price. I conducted a factory reset and rooted the phone. I removed all Samsung and Verizon bloatware. I purchased a T-Mobile SIM card and activated the hidden plan as discussed in this chapter.

Next, I secured the data traffic by installing a Virtual Private Network (VPN). Basically, it encrypts the network traffic, whether through cellular or Wi-Fi, for all data transmitted to or from the device. For this specific installation, I chose VyprVPN as the provider. This will prevent the cellular provider from having the ability to intercept the data or implant data packets with tracking codes.

The hidden T-Mobile plan includes only 100 minutes of talk time. For many, that is plenty. Most use the unlimited text and data for communication. However, it is important to have options for placing outgoing calls and accepting incoming calls that do not count toward this limit. In order to subsidize voice calling features, and add another layer of anonymity, I added two additional free telephone lines to the phone.

Google Voice

First, I installed the Google Voice app. Many readers just cringed when they read that line, but hear me out. Yes, I know that Google analyzes all of our data and uses it to generate targeted ads. I also suspect that Google stores every bit of data possible from its users. However, they offer a free product that will work well for my needs. Google Voice was discussed early while preparing for your journey into anonymity. The account referenced earlier is only to be used during the removal stage when needed. I created this second account for the sole purpose of making calls.

I created a new account while connected to a public Wi-Fi at a library, used the name of an alias, and selected a number from a different area code. Will Google still collect data on this account? Yes. Will they know it is you? No. Not if you are careful. You can use the Google Voice app to send and receive unlimited text messages. Please note that while you can delete messages within the app, it does not delete them from the “Trash”. You will need to access this account from a

web browser in order to properly delete messages from the account.

Hangouts Dialer

Next, I downloaded the Google Hangout Dialer app. This will allow you to make free calls from your device, using your data connection, without sacrificing any talk minutes. The calls will appear to come from your Google Voice number. This solves the problem of free outgoing telephone calls, but not the issue of incoming calls. If someone calls your Google Voice number, they will either be forwarded to your real cellular number (not recommended), or voicemail (recommended). This will vary based on your user settings. Instead, I will use another service to fill this void.

Groove IP / Ring.to

I installed GrooveIP to the Android device. This app, with the help of a Voice Over IP (VOIP) service called Ring.To, will give you unlimited free calls to or from your device. While installing the app is very straight forward, creating a new account can be a bit tricky. The most important rule with this technique is to conduct all actions over the device. Navigating to the Ring.To website and creating an account will typically result in failure. You can successfully create the account, but it will default to a premium paid account that you do not want. Instead, simply launch the GrooveIP app and follow the prompts to create a new account within the application. You will need to provide an email address that you can access and any desired alias name.

The email address that you choose must be associated with the telephone that you are using during registration. Navigate to Settings > Accounts > Add Account and provide the email credentials of the anonymous account that you will be using. In my experience, Gmail accounts work best. I created a Gmail account in an alias name, associated it with the device, completed the GrooveIP setup, and finally disconnected the Gmail account through these same settings. Before disconnecting the email account, you will be allowed to choose an area code and select a free telephone number within GrooveIP. This number will be assigned only for your use.

This phone can now open the GrooveIP app and place unlimited outgoing calls. These calls will appear to come from the new number assigned to the device. The calls will not use any of the cellular provider's minutes, and they will use the data connection to complete the call. If the app is open, the phone can accept incoming calls to this new number. There is no access to text messaging for this number.

I should summarize my current setup at this point. I have a cellular phone that is registered to an anonymous alias. The phone never makes or receives any calls through the carrier. A Google Voice account is attached to the device and that number can be used to make unlimited outgoing calls through the Hangouts dialer. A third telephone number can be used for incoming and outgoing calls through the data connection and GrooveIP. There are three individual telephone numbers at the user's disposal at any time. None of them are associated with a real name.

Many readers are likely wondering if they can have multiple numbers through these services on the same device. The answer is yes. You can log out of your Google Voice account at any time and login to another account. You are only limited by the number of accounts that you can successfully create. This also is true for GrooveIP. If you can successfully create an account through the GrooveIP app, using a new email address associated with your device, you can switch between the accounts and possess several potential cellular numbers. The headache will be the logging in and out process each time but this can be eased through the use of a password manager.

All of these services are free. There are also paid options that are very affordable that may give you a better layer of anonymity. These include popular services called Blur and Burner. My client wanted numerous options at all times, so I installed both to the device.

Burner

Burner allows you to create semi-anonymous, disposable phone numbers. These numbers can send and receive calls without requiring you to give out your real phone number. If you need to make a call or give out a number, you set up a new "burner". You can choose your area code and "size" of the burner you need. The

size is determined by how many days it lasts before self-destructing, how many texts and voice minutes are allowed, and whether or not it can send and receive photos. The burner will be created and you can then send and receive calls at this number.

My client can now use Burner while selling an item on Craigslist or some other classified ad service, giving a number to a new acquaintance or romantic interest who is not yet fully trusted, or signing up for a service that requires a valid phone number. These are all good opportunities to give out a number that can easily be terminated. If you wish to terminate the number before it expires, you can simply “burn” it on command. Alternatively, if you run out of texts or minutes or want to keep the burner longer, you can always replenish it inside the app.

One minor problem that I have repeatedly encountered with Burner is that it is very difficult to answer an incoming call. When you answer the call, you are greeted with a voice prompt that asks you to press “1” to accept the call. All of this takes time. Typically, when I receive a call on a Burner number, the other party has hung up by the time I finally answer. However, one area that Burner is extremely useful in is for receiving incoming text messages. If you want to set up a new email address, Amazon account, or other service that requires a working a text capable number, you can quickly set up a Burner number. This provides a decent layer of privacy between your true number and the account. This is the primary reason I choose to include this app.

Burner is a free app and comes with one free burner that is active for seven days. You can burn it sooner or extend it if desired. Burner uses your phone minutes rather than data, and can send and receive calls and texts. It also accepts voicemails. 25 Burner credits can be purchased within the app for $11.99. Burner lines cost from 3 to 8 credits each depending on the length of time they last. All burners will self-destruct after a given length of time if they are not renewed.

Blur

Blur was mentioned earlier when explaining masked email addresses and credit card numbers. Another privacy related service they offer is masked telephone

numbers. This feature allows you to create a phone number which you can send and receive calls. When you create a masked phone number, it forwards calls to your real phone number (or Google Voice or Silent Circle number), protecting the “real” number. There are a couple of minor downsides to this service. Although you can change the number to which your masked number forwards, there is a $7 charge to change the masked number itself. In order to place an outgoing call you must use the Blur app or login through your web browser. You will then receive a call from your Blur number. Once Blur has established a connection with you, Blur places the call to the third-party you are calling. It is not the most elegant solution but it could be used for things like verification and two-factor authentication text messages.

For most of Blur’s services there is no additional charge, but the Masked Phone charges a very reasonable fee of one cent per incoming call, one cent per minute the call is connected, and one cent per incoming text. Currently Blur’s Masked Phone service does not offer outgoing text messages. Your premium account will include a $3.00 balance to cover these charges. It should be noted that none of these solutions provide any type of encryption. Providers of these services could likely see the content of your calls.

At this point, my client is ready for fairly anonymous telephone calls and text messages. However, standard searching on the device could easily be captured by Google. Google wants to know what you search in order to build a dossier on you. This information will help with targeted ads. If intercepted by someone, this data could expose sensitive details about you. Please pause for a moment and think about everything you have ever searched on the internet. I previously explained a browser extension called Disconnect Search that eliminates this intrusion. That service has an app that will do the same thing. I installed this app on the client’s home screen and directed him to use this as he would use Google.

This phone provided a private environment for standard communication. The client could make outgoing calls from one of three anonymous numbers. He could receive calls from two different numbers. He could send and receive text messages from two unique telephone numbers.

Balance Refilling

In the previous example, my client chose to use T-Mobile as his cellular provider. The Amazon starter pack with SIM card also provided him his first month of service. At the end of that month, he will need to refill his account. Regardless of the carrier that you choose, it is important to refill the account balance as anonymously as possible. There are several ways to this.

- ✓ The easiest and most anonymous way is to purchase renewal cards with cash. These are often found on the end of an aisle in a store. There is usually a large rack of what appears to be gift cards for various cellular providers in increments of $30-$100. After purchasing, the card is activated and the credit can be transferred to your account online.

- ✓ The way recommended by most carriers to reload your balance is through an online payment via credit card. This can be acceptable if using Blur to mask your identity. I believe that cash in person trumps this option.

- ✓ If choosing T-Mobile, you could purchase additional SIM starter packs. Each of these includes the $30 credit that can be applied to an existing account. This method is often more affordable than cash when you consider the taxes added at checkout. Also, this idea may have more value when you read about my next client.

Wi-Fi Only

You may have noticed that the majority of the services that I recommend do not necessarily require a cellular service provider. They only require internet access through cellular data or Wi-Fi data. If desired, you could eliminate the activation of cellular service and rely on wireless internet. The pitfall in this plan is that your device will be useless for communication when you cannot find open access.

I always keep two devices operational at all times. My primary device possesses cellular connectivity and the secondary device only contains a Wi-Fi connection. While the setup for the secondary device is very similar to the primary unit,

there are a few differences.

- ✓ My secondary phones never attach to a wireless internet connection that I use with my primary devices or laptops. This prevents me from creating an association between the two devices. If I logged into two Google Voice accounts, on two unique devices, from the same network, Google would now know that I am the same person on both accounts. This may seem like overkill, and may not apply to your desired level of privacy.

- ✓ The secondary device possesses a Google account that was not created on a network connection that my primary devices access. Again, this creates a trail to the primary unit. I use public Wi-Fi to create, activate, and connect these accounts directly from my secondary devices. While this seems careless in regards to security, it is optimal for secondary devices that you do not want associated with your real identity.

- ✓ The secondary phone remains turned completely off until needed. It is always in airplane mode with the Wi-Fi enabled. All location services are disabled. These actions prevent your movements from being collected and stored.

- ✓ Finally, for the truly paranoid, I always turn my primary devices off before turning the secondary device on. I also confess that I do this while in motion so that the secondary device is not turned on at the same location the primary was powered down. Again, this prevents Google from knowing that I may be the same person using these two accounts.

iPhone

I have had clients that prefer to use an iPhone instead of Android. While I am comfortable rooting Android phones, I recommend against privilege escalation on the iPhone, also known as “jailbreaking”. Apple has taken a very pro-privacy, pro-security stance on behalf of its users and the overall security of the iPhone is

excellent. Apple does not monetize bulk data, and apps must be approved before inclusion it the curated App Store. Though some bad apps have been allowed into the app store, malware for non-jailbroken iOS devices is virtually non-existent. Further, most of the benefits of jailbreaking are in the interest of user experience and do not improve privacy or security. I believe iOS is a very secure mainstream mobile operating system and modifying it has a negative impact on privacy and security.

Had my client preferred an iOS device, a similar end result could have been achieved. Google Voice is supported on the iPhone through Google's own Google Voice app and through more functional third-party apps like GV Mobile+. Unfortunately, GrooveIP is not available on iOS devices. However, a user has the option of using multiple Google Voice accounts on a single device if he or she is willing to log in and out of the accounts. Additionally, iOS users can use Burner to provide unlimited inexpensive and disposable numbers.

As I have mentioned previously, privacy is not cheap. If you are willing to pay, there are numerous apps that allow you to have a second phone line on your iPhone. My favorite is called Line2. Line2 is a voice-over IP (VOIP) cross-platform app. You can use it on your iOS, Android, Mac, or Windows device. Line2 works over 3G, 4G, LTE, and Wi-Fi. The downside of Line2 is the cost of $9.99 per month.

iCloud/iTunes

Choosing to use an iOS device will also necessitate having an iTunes and iCloud account, without which you will be unable to download applications. Though Apple does not monetize data, and the iAds program through which app developers can monetize apps can be opted out of, I still prefer to store as little information in the cloud as possible. For this reason, I back nothing up to iCloud. To gain full use of an iTunes account, you will have to provide a credit card number. In the interest of setting the account up as anonymously as possible, I recommend the following technique:

- ✓ Do not provide any real information to Apple when setting up the account. Choose an alias name that you will be comfortably using for some time. I choose names associated with devices such as MacBook

Air 2015.

- ✓ Log into Blur and create a masked credit card number in a small amount. The amount is up to you, but I recommend a minimum of $10.

- ✓ Use this credit card number to purchase an app, song, or other product from Apple. This well establish the card as valid.

- ✓ Go to a brick and mortar store and purchase an iTunes gift card in an amount you will not exceed in the immediate future. I recommend approximately $25 if you are a very light user of iTunes and $100-200 if you are an average to heavy user of the service.

- ✓ Maintain a gift card balance. As long as you do not use or exceed the balance, iTunes should never attempt to withdraw money from your credit card, preventing you from having to purchase a new masked card.

Extreme Anonymity

I recently had a client in a unique situation. He was a high level CEO that believed sophisticated hackers were targeting him at the direction of a competitor. He had received several text messages with links to malicious websites attempting to compromise his device. It was vital that his daily telecommunications were anonymous. He was not technically sophisticated and did not desire third party applications to make calls over data. His request was very simple at first. He wanted an anonymous cell phone for data and text. He would be making no voice calls. The additional demand was that he wanted to be issued a new telephone number and account every month, and would never use the same data plan for more than 30 days. He believed that having a new number every month would make it more difficult to target his account.

- ✓ I created a Blur account for him and attached a secondary credit card in the name of an assistant that could receive mail at a PO Box.

- ✓ I created twelve masked Blur credit cards with a balance of $30.95 each.

- ✓ I created twelve Amazon accounts in the assistant's name. With each account, I ordered one T-Mobile SIM starter pack using a different masked Blur card for each purchase.

- ✓ I obtained a slightly used iPhone that would work on the T-Mobile network.

- ✓ When the SIM starter packs arrived, I labeled them each by the month that they would be used. Every 30 days, the client would allow the prepaid account to expire. I would then insert the next card and follow the very simple instructions to activate the next SIM card. He would repeat this process every 30 days.

- ✓ Every time his plan expired and he activated a new card his phone number would technically change. But because he was using VOIP solutions and never gave out the T-Mobile number to anyone, the change was completely transparent to his contacts. The only additional step he had to take was to log into his Google Voice account and change the number to which his Google Voice number forwarded.

I respect that there are privacy flaws with this plan. T-Mobile would be able to see the hardware information (IMEI) from the device and would know that this was likely the same person each month. However, they have no reason to look. Is this overkill? Quite possibly. However, the cost was minimal. It would have been the same price to purchase the first card and refill the balance monthly as it was to issue a new SIM card every month.

An additional benefit is that each account that expires can be refilled within five months of expiration. In other words, you can allow your balance to deplete at any time. The account will stay there for you up to five months in a dormant state. At any time, you can reactivate the account by adding the standard $30 monthly usage fee. Your same telephone number will be activated on that SIM

card. I know of no traditional cellular plans that will allow this type of flexibility.

With this plan, you could own a new cellular number and online account every month. If you use VOIP services as your primary number, this would have no negative impact on your daily communications. If you open numerous social network accounts that each require a unique cellular number for verification, this method has huge potential. It would allow you to provide your actual cellular number while knowing that it will be disconnected in one month. I am not personally comfortable with this because the number is attached to a device that knows your location for the past month. It will depend on your level of paranoia.

The Complete Reset

My favorite clients are those that want a complete reset of their entire communications strategy. They realize that they have been sharing intimate details with huge corporations and jeopardizing their privacy every time they looked at their phone. They understand that every movement of theirs over the past several years has been tracked, logged, and preserved thanks to the device carried in their pocket or purse. While the previous examples illustrate good privacy protocols, I had a client that wanted to take it further. The following scenario occurred in early 2015. The sharing of this content was approved by the client in hopes that it may help someone else.

“David” was a government employee under attack by a group of very sophisticated hackers. He was confident that his personal email account and cell phone had been compromised at some point. Sensitive details about an investigation were leaked during a trial which were only present in private email messages. He met with me and provided his device.

I analyzed his personal cell phone and discovered several suspicious text messages that appeared to contain malicious website links. David believes that he may have clicked one of these many weeks earlier. I observed that he used Gmail as his personal email account and his email address included his real name. A quick search online found this email address present on many websites. I also confirmed that he used his personal cell number on his Facebook page and that it was visible to any “friends”. These presented two very large attack surfaces.

I informed him that he should never use this telephone, number, or email account ever again. Attacks will likely continue toward these accounts and he must assume that the device is compromised. David was ready to commit to starting over but had a few reservations. He asked that he could still somehow see any communications going to his old accounts while being safe with only new accounts associated with a new device. I began my assignment.

I purchased David a brand new telephone. He insisted on a device that had never been assigned to anyone else. I chose the third edition of the Motorola “Moto G”. This phone had a stock Android operating system, no bloatware, and is unlocked for any GSM network. It was also only $179 without any contract. I purchased the device through Amazon, with an account in an alias name, using a pre-paid Blur credit card attached to another alias name, shipped to a mail drop registered to a friend with a very common name.

I activated this device with an anonymous T-Mobile SIM starter pack purchased previously with Vanilla Visa prepaid cards. I refer to these SIM packs as “Shelf SIMs”. I usually have about 30 ready to go at any time. This presented him with a brand new phone and private cellular number. Neither is connected to him in any way. The activation was completed from a café in another city on a Wi-Fi connection through a VPN. The phone was registered to a generic name.

The Android phone must be connected to a Google account in order to properly function and connect to the Google Play store for apps. I created a generic Google account through another anonymous internet connection that had no association with his real name. This account will never be accessed from a computer. The attack surface of this device is extremely minimal because there is no affiliation to David.

I exported the entire contents of David’s Gmail account and then deleted all messages within the account. If the hackers still had access to this account, the data is gone. He chose a new non-Gmail email provider and I imported all of his messages into that account. I installed the official Android application for that email provider and connected his account. All of his email was now available to him on his device without any connection to the old account. However, any outgoing messages were now routing through the new email address.

David expected that he would need any email still being received at his previous Gmail account. I set up a rule within his old Gmail account to forward all incoming messages to a new 33 Mail account created for this purpose. The 33 Mail account was configured to forward these messages to David's new personal email account. If hackers were able to access David's old Gmail account, they could see the forwarding address. If a Google employee was ordered to find any forwarding information, the 33 Mail account is all that would be seen. The 33 Mail address does not compromise David's new email address. I set up a rule within David's new email account to forward all messages from 33 Mail into a folder titled "Caution". This would remind him to be careful when viewing these messages.

David requested that his contacts be imported from his old phone into the new device. This is where I drew the line. If I were to import the hundreds of contacts from one account into another, I would create an obvious connection between the accounts. Google would begin to recommend apps based on his "friends" and would know a lot about David. I asked him to revisit his contacts while logged into his Gmail account through a laptop. He discovered that Google had been automatically populating information into his contact list every time he sent an email to someone. Google then used data from Google+ to create profiles on each contact. David had over 4,000 people in his Google contact list.

The current view of Google Contacts does not isolate intentional contacts from automatically populated profiles. Fortunately, the previous version of Google Contacts allows this separation. While viewing the current version of these contacts, I navigated to https://www.google.com/contacts/u/0/?cplus=0#contacts. This loaded the previous version of the contacts database which includes "My Contacts" and "Other Contacts". In David's scenario, the "My Contacts" included 217 people while the "Other Contacts" included over 4,000 people.

I first exported the entire contact list before taking any action. On this previous view page, I chose "Other Contacts", then "More", then "Export". I exported all categories of contacts into a standard CSV file. This could be later imported into an email client if a contact's information was needed.

I then deleted the entire "Other Contacts" category and allowed David time to consider the remaining 217 contacts. Many of these were people that he no

longer communicated with. I encouraged him to only save the contacts that he would need to communicate with via phone from this new device. These should only be close friends and family that he would be comfortable reaching out to if he needed some type of help. The final list included 28 people. I then exported only this list for import into the new device.

Before import, I opened this exported spreadsheet file with Microsoft Excel. The file was organized into columns including first name, last name, mobile number, and others. I focused on the name sections and asked David if possessing the full first and last name was vital to him. Since he was being heavily targeted by sophisticated criminals, I encouraged him to not include the full names of his contacts in his phone. If he were compromised again, this information could put others in danger. He agreed to use only initials for most of the contacts. For those that would create duplicate initials, he chose a city to help identify the options. One example might be T S (Denver) while another is T S (NYC). While the name of the friend is not disclosed, he would know right away which contact he desired.

This technique may have brought out a laugh or an eye roll when read. I agree that it might be overkill for some readers. However, my entire contact lists on my devices contain absolutely no names. I believe that this method decreases future attack surfaces while protecting both myself and my contacts. It prevents Google or other services from extracting any details provided by me to their profiles on these people. While I crave the dated methods of storing contacts into a flip phone without internet access, I accept the digital world that I live in today. David’s personal life with his friends and family is now more secure by changing his phone habits.

David had previously used Google Calendar for all of his appointments. He stated that it was crucial to maintain this setup. His configuration had two calendars. The first was the default personal calendar and the second was marked “Private”. He stated that he only wanted the personal calendar, so I exported the iCal file and properly deleted all of the entries. Through his Google account, his personal calendar was now empty. However, there were several sensitive entries associated with the “Private” calendar. David asked for a few minutes to look through these in private.

David returned and said that he did not need the “Private” calendar and that he had deleted the entries. When asked for clarification, he confirmed that he had “Unsubscribed” from the calendar and that it was no longer visible. Unfortunately, this does not delete anything from Google. That calendar was still present in their system and the content was visible to anyone at Google. This put David into a slight panic. Fortunately, there is always a way around these things.

This calendar was associated with the same Google account as his Gmail. I had David’s entire Gmail account backed up as a 5GB file. I expanded the data and conducted a search for group.calendar.google.com. Every Google calendar has a unique ID that ends in that address. I quickly located an email message notifying David of a change to an entry in the “Private” calendar. These are common when appointments are entered and later changed. They are considered notifications. Within that message was an attachment titled “Attachment1.3”. This was a small text file with data similar to the following.

ORGANIZER;CN=ORGANIZER;CN=Private:mailto:u8%rsg79dqbdtvjdi88&6@group.calendar.google.cor

The unique address listed after “Private” is the ID for that calendar. I connected to his old Google account, clicked “Settings”, clicked “Calendars”, clicked “Browse Interesting Calendars”, clicked “Add a friend’s calendar”, and provided the address in the attachment. This populated all of the “Private” entries back into his calendar. This was proof that unsubscribing to a calendar does not delete any data. In the settings for this calendar, I chose “Permanently delete this calendar”. The data was now gone.

David had previously used a Google Voice account for all of his text messaging. I configured his account to forward all incoming messages to David’s 33 Mail account. This will allow him to see any incoming texts through his new email account in the “Caution” folder. If he chooses, he can reply through his new Google Voice account.

I created the Google Voice account while in the café mentioned previously. Google demanded a valid telephone number in order to activate the account. I told the barista that I was trying to connect to a webinar, but that I needed to validate the connection. I asked if I could use their phone to accept a brief incoming call in order to enter a code to prove that I was human. I was allowed

and give Google Voice the number of the café. Google presented a code on the screen and the café phone rang. I answered, entered the code when prompted, and then possessed an active Google Voice account. All I had to do then was to select a new phone number.

I then changed the password and enabled two-factor authentication on both the old and new Google accounts. David should rarely need to access either. The Gmail and Calendar accounts were free of any personal data. David stated that he would never use the telephone number assigned to his new device. Instead, he would use GrooveIP for incoming and outgoing calls and his new Google Voice number for text messages to the trusted people in his life. It will be very difficult for anyone to determine the phone that David uses every day. Tracking him through this device is not likely.

If David were worried about physical monitoring of his device while in the vicinity of his location, I would encourage appropriate security habits. I have instructed other clients to turn the telephone completely off while traveling close to their home. In one scenario, a client always turned her phone off at a specific landmark on her way home from work. The next day, she would turn it back on at that same landmark while on her way back to work. If anyone were to identify and scrutinize her cellular account, it would have no location information about her residence. Additionally, she never needed her phone while at home. She used an anonymous Google account for all phone calls from her computer.

I took great care in the actions executed for David. More importantly, I was careful to avoid taking any actions that could compromise the situation. Instead of focusing on the details that were performed, it may be more vital to review steps that were NOT taken.

- ✓ The Google accounts were not created on the same computer as the client's real accounts. Google cannot use browser fingerprinting to pair the two.

- ✓ The Google accounts were not created using the same IP address of personal accounts. IP logs would not compromise the accounts.

- ✓ The Google accounts were never accessed from the same connections as personal accounts. IP logs at Google would not disclose the connection.

- ✓ The telephone account was not activated using internet connections associated with the client. The cellular provider cannot associate the account to the client.

- ✓ The telephone was not connected to any accounts associated with the client. Neither the cellular provider nor Google has any connection to the client.

- ✓ The telephone was never connected to any Wi-Fi access points associated with the client. Google cannot use their Wi-Fi database to make the association.

- ✓ Various personal accounts were not imported into the new telephone. Google cannot use historic data to associate the new phone to my client.

Is this all overkill? Some may think so. However, my experience supports my paranoia. I have witnessed investigations involving Google and other similar companies. They know more than you think. They know that you have multiple Gmail accounts under various names. They record this activity and will disclose all of your related accounts if given an appropriate order. More concerning is when their data is compromised during a breach and all collected information is exposed. Some may read this and think that it will never happen. I am sure that the 32 million subscribers to the marital affair website Ashley Madison assumed they were protected as well. They were not.

Why can't I give my cellular number to close friends and family?

During my trainings, I have learned that most users possess a single cellular telephone number and use it for all voice communications. I believe that this is very inappropriate behavior if privacy is desired. The following will identify the four main concerns.

Attack Surface: As said before, if your publicly known number is your actual cellular number, you have created a direct link to your cellular account. If this account is compromised, it contains data about your historical locations and communications. It is also possible for anyone having access to your mobile phone account to set up SMS forwarding. They could use this to forward your two-factor authentication tokens to their device to get into other online accounts. If someone only knows your VOIP number, it is not always possible to associate that number with a cellular account. By using a VOIP number, you have created a layer of protection from revealing your cellular account.

Dynamic Number: If you rely on VOIP methods for communication, you can easily activate a new cellular account at any time without notification to your contacts. You can change cellular providers, hardware, and calling plans at will, and never have to update your information with anyone. You can link the known VOIP number to any cellular plan without anyone noticing a difference.

Verification Mechanism: In some cases your phone number is a verification mechanism. For example, if you call your bank you may be told “we see you are calling from the primary number on your account” and face fewer security questions as a result. It is possible for someone who knows your cellular number to spoof it and call the bank, pretending to be you. I recommend using a VOIP number for your financial institutions, but a different one than you give friends and family. If you only give this number to banks it will be very difficult for anyone to find.

Account Privacy: The most vital reason for never giving your true cellular number out is to keep it private. In past years, there were no cellular number lookup websites or publicly available databases of all cellular owners. Today, this exists. You also need to be aware of sites such as TrueCaller. This is a crowd-sourced telephone directory that will display a real name for most cellular numbers. It works as an app that a person installs on their device in order to see caller ID information when receiving a call. What most people do not realize is that the app also collects all of your contacts, including name and number, and adds them to the live online database. As of this writing, my disconnected government issued cellular number can be searched on this website to reveal the true name associated. This is because someone that I know downloaded TrueCaller and unknowingly shared all of their contacts with the world. Further,

they are sharing your true cellular number and name with either Google, Apple, or Microsoft, depending on the device operating system. Their account likely syncs several times every hour. Can you hold complete trust in the security and ethics of any large corporation? I believe not.

I often encounter skeptics that ask me “What is wrong with having a contract for cellular service like everyone else?”. My response includes several levels of concern, most of which have been outlined in this chapter. Overall there are two main vulnerabilities. The first is associated with privacy and the second security.

As I have displayed in this chapter, you lose all privacy when you register a phone in your real name. Because of the subsidies offered to you in the form of discounted phones, you will be required to also disclose your DOB and SSN for credit checks. Your identifiers, phone, account, number, calls, texts, location, traffic, and overall usage will be forever stored. It will be disclosed to anyone that possesses a court order for the data. It can be extracted by any rogue employee of the provider. Criminal hackers will access any data from illegal breaches.

For those that do not care to protect this data, or subscribe to the “I have nothing to hide” mentality, I offer the following. As I write this paragraph, T-Mobile has announced that 15 million customers’ data were exposed during a breach through Experian, a vendor they use for credit checks. This means that 15 million T-Mobile customers that used their real information are compromised. Their names, addresses, account data, and SSN’s are now in the hands of unknown hackers. I see no scenario where this is not a concern to most. While I have T-Mobile accounts, I have no concerns. The accounts have absolutely no information about my true identity. They do not possess my name, address, SSN, or credit card number.

Additionally, there are several news sources citing a new vulnerability in Android that allows the device to be compromised by simply receiving a malicious text message. This message contains specific coding that infects the phone with minimal input from the user. I believe that by eliminating the telephone number of your device from your attack surface, you are well protected from this issue. If you never give out your actual cell number, and only use the text message alternatives that I have described, you will not fall victim to

this attack. No one will know the number that they need to target. In the worst case scenario, you will receive these messages within accounts such as Google Voice. Without going directly to your stock messaging app on your phone, these attempts are useless.

Encrypted Communications

This chapter would not be complete without discussing encrypted communications. While most of the communication tools that have been mentioned here are technically encrypted, they do not protect you from unauthorized view. The text message that you send through your cellular provider is encrypted in transmission, but likely stored in plain text on their servers. The Google Voice text message that you send through their app is encrypted in storage, but Google has unlimited access to the content. These services protect your communications from public viewing, but the providers can see everything. You may desire more sophisticated software. I will discuss three services that will cover all of your encrypted communication needs. In the following examples, the providers encrypt all communications and cannot see any of your content. If they were ordered to release their data, it would be useless to anyone. It would appear as a mess of random data and would reveal no personal information. As you will see in my upcoming telephone strategy, I rely on these apps daily. I always use this type of messaging whenever possible.

Signal (whispersystems.org)

Signal Private Messenger is a free application. It supports both voice calls and text messaging in a single app and is incredibly easy to use. There is no complicated setup, no username or password to create and remember, and the app is incredibly intuitive. It resembles native phone and texting applications. Signal uses your phone's Wi-Fi or data connection. To use Signal, simply install the application. You will be prompted to enter your telephone number for verification, and a Google Voice is acceptable. The app will verify the number by sending you a code that you must enter into the application. No other personal information is required or requested. If you allow Signal to access your contacts, it will identify those who have Signal installed. I recommend setting up a Google Voice number that is used only for Signal, and giving that number out to friend, family, and business contacts that are likely to use Signal. If you are

not planning to change your number or transition to Google Voice, then you should register Signal with your existing number.

The call and text interface will display two random words. The words displayed will change with each phone call but should match on both handsets involved in the call. These words are used to ensure the call is not being tampered with by a man-in-the-middle attack. If an attacker were to successfully intercept a call, each handset would establish a key with the attacker rather than the corresponding handset, and each phone would display different authentication words. I recommend validating these words at the beginning of each conversation made over Signal, and especially before engaging in sensitive communications.

Silent Phone (silentcircle.com)

Silent Phone is probably one of the most widely publicized encrypted voice applications in existence. Its parent company, Silent Circle, is well-known in the security and privacy arena for their custom BlackPhone handset. The app is free to download, but you must pay for a subscription before you can use it. Silent Circle offers several subscription plans. The first, and least expensive at $10 per month, is called “Silent Suite”. Silent Suite allows you unlimited encrypted voice and text communication with other Silent Circle users.

The next level of subscription, Silent World, permits you to call any landline or mobile numbers. Silent World also gives you a telephone number that allows you to receive incoming calls from any landline or mobile number. I can now have an incoming and outgoing phone number that works in most countries. The major benefit of this number is encryption. When you place a call with Silent Phone, it first goes to a Silent Circle server where an encrypted connection is established. Traffic between the server and the person you are calling is not encrypted, but it does ensure that any local cell site simulator will not intercept the communication.

Wickr (wickr.com)

Wickr is a free mobile app that can also be used as a desktop messaging

application on Windows, Mac OS X, and Linux operating systems. After downloading the Wickr app to your device, you must choose a username and create a password. Wickr asks you for no personal information during setup. Once the username is activated, users can message each other through the interface. Wickr can also be used to securely send pictures, videos, voice messages, and attachments from Dropbox and Google Drive. According to the company's privacy policy, Wickr messages are only stored on the servers in an encrypted format and are stored until the message has been delivered. After delivery, the messages are securely erased from the servers.

Wickr is considered an ephemeral messaging service because your messages are deleted from both the sender and recipient's devices at a set interval of your choosing. I usually choose a one-hour interval. You should be aware that users do have the ability to take screenshots of your text messages and photos. To be fair, anyone could also capture a photo with a second device without alerting anyone. This should be used with people you trust.

Which should you use? It will depend on your situation. If you only use a mobile device for texts and calls, Signal is probably all that you need. If you want secure messaging from a computer to other people's devices, Wickr may work better for you. If you desire secure communications over standard telephone calls, a paid Silent Circle account will be required. The following page contains the details of my personal communications strategy. After, are two blank templates for you. They can be used to strategize or document your plans for creating anonymous devices.

This chapter may have quickly turned into an advanced level for many readers. I believe that knowing about all of your options will help you make the most appropriate decision for your situation. What works well for a domestic violence victim might not be enough for a targeted special operations individual. The design for a covert agent may be overkill for a civilian privacy enthusiast. Fortunately, the majority of tools are free and at your disposal. I suggest that you try them all and see what works best for you.

My Mobile Communications Strategy

Primary Device

Hardware: BlackPhone 2
Operating System: SilentOS (Android 5)
Carrier: T-Mobile
Plan: $30 “Hidden” Prepaid, 100 Talk, Unlimited Text & Data
Primary Alias Incoming/Outgoing Calls: GrooveIP
Secondary Alias Outgoing Calls: Google Voice (Hangouts Dialer)
Secure Personal Incoming/Outgoing Calls: Silent Circle / Signal
Primary Alias Text Messaging: Google Voice
Secure Personal Text Messaging: Wickr / Silent Text / Signal
Secure Personal Email: ProtonMail
VPN: PIA **Password Manager**: Keepass **Encryption**: SilentOS Default

Notes: I alternate between two T-Mobile SIM cards. When I am home for an extended period of time, I use my primary SIM. When I prepare to travel for extended time, I allow the primary to expire and I activate the secondary SIM. This way, I am still paying the typical $30 monthly fee, but I can switch the accounts every other month in order to avoid tracking of every movement. There is crossover from home to travel, but an analysis of any one of these accounts would be missing a lot of data about me. Of course, knowing both of my accounts would tell the full story. Each account is in a different alias. One is always paid by Blur masked numbers, and the other only with cash refill cards.

Secondary Device

Hardware: Samsung Galaxy S3
Operating System: Android KitKat (Rooted)
Carrier: None
Plan: None (Wi-Fi Only)
Primary Alias Incoming/Outgoing Calls: GrooveIP
Secondary Alias Outgoing Calls: Google Voice (Hangouts Dialer)
Primary Alias Text Messaging: Google Voice
Secure Text Messaging: Wickr / Signal
Secure Email: ProtonMail
VPN: PIA **Password Manager**: None **Encryption**: Android Stock

Notes: This phone is turned off at all times unless needed. I carry it with me while traveling when I need to make or accept a call or text while acting as an alias. This device is used for Uber and other invasive apps when necessary while traveling. If I need to connect to any public Wi-Fi, it is from this phone, and never my primary.

Your Mobile Communications Strategy

Primary Device

Hardware: _____

Operating System: _____

Carrier: _____

Plan: _____

Primary Alias Incoming/Outgoing Calls: _____

Secondary Alias Outgoing Calls: _____

Secure Personal Incoming/Outgoing Calls: _____

Primary Alias Text Messaging: _____

Secure Personal Text Messaging: _____

Secure Personal Email: _____

VPN: _____

Password Manager: _____

Encryption: _____

Notes:

Your Mobile Communications Strategy

Secondary Device

Hardware: _____

Operating System: _____

Carrier: _____

Plan: _____

Primary Alias Incoming/Outgoing Calls: _____

Secondary Alias Outgoing Calls: _____

Secure Personal Incoming/Outgoing Calls: _____

Primary Alias Text Messaging: _____

Secure Personal Text Messaging: _____

Secure Personal Email: _____

VPN: _____

Password Manager: _____

Encryption: _____

Notes:

Chapter Eight

Personal Data Removal

The removal process of your information is usually easy, with a few exceptions. Most services will offer you a website to request they remove your details. These direct links are often hidden within fine print or rarely visited pages. My goal in this chapter is to take the research out of the removal process and simply tell you where to start. Many of the links listed here are long and easily mistyped. I encourage you to visit the resources section of my website. As mentioned before, the link called “Privacy” will have everything you need.

The first two editions of this book outlined specific details of the data removal process for each service that was mentioned. It also included screen captures displaying the process. Since its original release in 2012, many new data collection companies have surfaced. Instead of explaining each step of the process for every service, I decided to compress this information throughout this chapter. I did not include any screen captures in order to provide removal details of every service that I could locate within the space limitations of the chapter. This section should be used as a workbook.

Each removal summary will display several pieces of information about each service that I have identified. The following structure outlines the data that is displayed throughout this chapter. The final line will have blank forms for you to document your work and successful removals.

Service: The name of the service **Category**: The type of website
Website: The website of the service
Removal Link: The direct link for online removal, if available
Privacy Policy: Page containing detailed instructions

Email Address: Any email addresses that will reach an employee responsible for removal
Requirements: Any special requirements, such as a copy of an ID or written request
Notes: Any special instructions
Date: (date of request)
Response: (response received)
Verified: (confirm removal)

The “Date” field should list the date that you submitted the removal request. The “Response” should include any details received from the service after your submission. The “Verified” option should be used to “check-off” that service after you have confirmed that your details have been removed. I recommend using a pencil. This will allow you to conduct this process repeatedly for family members and friends. 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 legal privacy policy, please remove the following details 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)

This chapter is displayed within five unique sections:

People & Telephone Search: Free websites that expose your home information.

Public Data Brokers: Companies that sell your data for public use.

Non-Public Data Brokers: Companies that sell your data for private use.

Data Marketers: Companies that collect and sell your interests for targeted marketing.

Ancestry Records: Services that display family information provided by users.

At the end of each section, I present the workbook portion that will help you issue your data removal requests. I recommend pursuing data removal in the section order presented. The most important may be people search databases.

People & Telephone Search Engines

When a person wants to locate your home address, telephone number, family information, or associations, he or she will probably visit an online people directory website. These sites give anyone with internet access a view into your personal details, often including your home address, telephone number, and family member's names. When we were young, the only option for this type of information was a phone book or community roster. If the subject of interest paid for an unlisted number, we were out of luck. Today, an unlisted number and address means nothing to the internet. Other sources, such as tax data, social networks, resumes, and marketing databases, fill in the gaps. The people and telephone search websites listed at the end of this section are mostly free to access. They create revenue by enticing visitors to pay for premium data in the form of a complete background check. These premium services are often disappointing.

Deleting Inaccurate Information

During your information deletion process, you are likely to locate inaccurate data. You may find a previous address or addresses where you no longer reside. Many privacy advocates encourage people to leave this information online to protect real addresses. This is an example of disinformation. I do not recommend

leaving any information online that was ever accurate. While the expired data may not be a privacy issue, it can create a serious security problem.

Many online services will require you to complete a questionnaire to confirm your identity. Common examples would be when you open a new bank account online or request a credit report. The questions generated during this automated process are validated through your current credit report and personal profile. These questions are designed to be difficult to answer by anyone except you. The questions usually reference previous addresses and the precise amount of specific bills. The following example illustrates how leaving your previous addresses online can jeopardize your identity.

An identity thief decides to open a new credit line in your name. He has already obtained your full name, date of birth, and social security number from various sources. He completes a form on a credit lender's website and is asked two security questions to verify the identity. Your security questions likely include a previous residence street and current home mortgage holder. This type of verification is common on financial websites. The multiple choices make it easy to guess the correct answer, but an educated thief will conduct a quick search. Searching the victim's name on Spokeo identifies a previous residence addresses with the numbers masked.

This scenario is far too common. This is why I recommend erasing all information from public view. An old address on a reverse search website can haunt you later. If you find information associated with you that has never been correct, you should leave it. If a people search website identifies your residence as a location where you have never lived, this can be beneficial. Disinformation is an effective privacy layer.

Do Not Call Registry

This is the most common opt-out request conducted by people. It adds your telephone number to a database of numbers that are passed on to telemarketing companies from the government. The companies are forced to remove these numbers from their automated systems used for telemarketing. This should stop unwanted sales calls and add an extremely thin layer of privacy for you. You can register landlines and cellular numbers, and it is recommended that you register

all numbers that you own.

- ✓ Navigate to donotcall.gov and click the “Register a Phone Number” button. Identify up to three telephone numbers that you want removed from telemarketers’ databases. Provide your anonymous email address and click “Submit”. Verify the information and again click “Submit”.

- ✓ Check your inbox. You will receive a separate message for each number that you registered. Click on the link in each message to confirm the removal request. You will be forwarded to confirmation that the number was entered into the registry.

Nomorobo

While the Do Not Call Registry will likely stop many of the undesired calls that you receive from telemarketers, it is not perfect. As a backup, consider registering with Nomorobo at nomorobo.com. You must provide your type of connection (cell, landline, VOIP), service provider, and telephone number. You must also provide a working email address, such as your anonymous personal account created earlier. Some carriers are not supported yet.

Landline Telephone Numbers

Telephone number directories are generally split into two categories, landline and cellular. The way that landline data is acquired is much different than cellular data. Much of the landline data is obtained from the companies that create phonebooks and city directories. This data originates with the telephone companies that provide the service. If you have a landline telephone at your house in your name, this information is available to the public. If your number is unlisted, that does not mean that it is not in public databases. In fact, most people with unlisted numbers are listed in the online directories mentioned in this chapter. This is because public information, such as voter records and tax data, leak telephone numbers into public databases. If your number is not listed as private, you should request this option with your telephone service provider.

During this contact with the telephone company, I recommend that you update your contact information with them. Once you have established service with the telephone company, there is no further need for them to verify your details and check your credit. You can now basically change your information to whatever you want. Obviously, the address of service must stay the same. However, you can change your billing address to your post office box address. This will eliminate your home address from a database that is shared for marketing purposes. Your bill will now be sent to the post office box.

Next, consider changing the name on the account. This cannot be a complete change, but changing a portion of the name will make your listing more difficult to find. For women, the easiest change would be your last name. Calling the telephone company and notifying them of a last name change is common. There is no verification process. Women may want to state that they were recently married and provide an inaccurate new last name. For men, consider a change of the spelling. I have found success with conversations using the following template.

“Hello, my name is Michael Bazzell, and I have service through your company. This really is not that big of a deal, but your contact information for me has my name spelled completely wrong, and I would like to finally correct your records. You have my first name as “Mike”, but it is actually “Michael” spelled M-I-C-H-E-L. My last name is spelled B-A-S-I-L. Could you correct the record?”

These corrections are made immediately and never verified. Now, the listing has your first and last name spelled incorrectly. You may wish to obscure your details even further by making incremental changes. For example, the follow month your wife or girlfriend could call and state the following: “my name is actually Michelle Basil. I know this is not a big deal but could you correct the spelling of my first name? The correct spelling is M-I-C-H-E-L-L-E.”

Now the name on the account is both misspelled, and of the opposite gender. Anyone researching your location will have difficulty finding this listing. Through persistence, creativity, and subtle, incremental changes you can eventually modify your name to something entirely different. If you receive an operator who will not change your name, hang up and try again. It is very likely that you will get a different operator. Through trial and error, you are almost

certain to find one who would be willing to change your name in the system.

Companies will probably acquire this data and continue to make new databases. This will not have a big impact on you since your last name is spelled differently or changed completely. You should now focus on removing the correct data from the internet.

Cellular Telephone Numbers

There are fewer cellular number directories than landline directories. There is no official White Pages style of phonebook for cellular numbers. That does not mean that the numbers are private. Many companies are attempting to create databases of cellular numbers and make them available to the masses. There are several methods they use to collect your number.

All of these databases rely on someone supplying a cellular number to them. Usually, this is you. When you use your cellular number as a contact for anything official, you take the chance of this number becoming public information. For example, when you sign up to win the new car at the mall and supply your name, number, and address, that information gets added to a large database. When you locate and print online coupons, you are often required to provide your personal information including a telephone number. This content also gets added to various databases. The advancements in technology allow for immediate identification of a telephone number to determine if it is a landline or cellular number. This identification can also be added to the database. A later chapter will discuss how you should protect this information in the future. Next are the methods for removing your cellular number from databases.

Caller ID Databases

You probably know that when you call a landline telephone number from your home landline service, you pass along the caller ID information about your account. If your home phone is registered in your name, your name will appear on the caller ID screen of the receiving telephone. Many people do not realize that the name associated with your cellular telephone is also provided to the receiver’s caller ID. Most cellular companies now announce your name and

number when you call landline telephones. You cannot stop this data from being transmitted, and this practice is acceptable to the telephone companies because you are generating the contact by placing the call. Only a few years ago, this would have been fairly safe. Today, anyone can look up your cellular number.

There is an abundance of reverse caller ID service providers that will allow anyone to identify the owner of a number for less than a penny. One service that currently offers a free trial of this type of query is Who Calld. Navigate to whocalld.com and search your cellular or landline number. If you do not see your name, click the “Update” button.

You will likely see your name and cellular service provider displayed publicly. Attempting the same search at numerous reverse caller ID providers will also likely present your name as associated with your cellular number. There is no point in contacting these providers and requesting removal. While some have this option, most do not. Additionally, your data will be repopulated soon by your cellular provider or another third party company. Instead, you should consider modifying the subscriber information on your account. The following true scenario should help guide you through your own process.

I conducted a search for a relative’s number through seven unique reverse caller ID services. All of them accurately identified her name as associated with her number. With permission, I logged into her online billing account and viewed her details. She was one of five members of a family plan with AT&T. Not only was AT&T providing the information of the subscriber, but also each individual name associated with each number on the family plan. I changed this relative’s name to “A. Unknown”. Within seven days, I conducted another query on her cellular number. The caller ID information associated with it was updated to “A Unknown”.

I conducted a search for a friend’s telephone number. I found that half of the online databases had her name listed correctly, while the other half had a different name that I will call “David Brown”. This name was consistent across all of the listings so I assumed it was the former owner of that number. With permission I logged into her Verizon Wireless account and changed her name on the account to that of the former account holder. Within fourteen days I conducted another search. All the queries returned either “David Brown” or “D

Brown". Her name was no longer associated with this number in any of the online databases.

You can likely log into your own online portal for your cellular account. If you are on a family plan, attempt to change the name as it appears for your individual number. If you are not within a family plan and have only one number on the account, attempt to change the name associated with the bill. Some services allow this activity through their website. If yours does not, consider calling them and specifically ask to change the information associated with your caller ID.

Other Online Directories

New websites promising accurate reverse telephone number information appear routinely. Some of these stick around and achieve slight growth, but most disappear or become unused. Those that are useful tend to become acquired by larger data companies. You should routinely conduct a search of your telephone number on Google and Bing to view the results. If you find too many spam results, try placing quotes around the number. If you find a website that has posted your personal information, start snooping around and try to find a link titled "Privacy" or "Terms of Service". These links identify the procedure for removing your information. If you cannot find them, there is one last thing to try.

Most data mining websites, including telephone directories, have established some type of policy that prohibits children from posting their information. If this information is identified by the company, a manual removal is conducted immediately. As an example, assume that you found your telephone number and address on the website cellrevealer.com. This site offers mediocre reverse cellular telephone number lookups. They do not have any sort of removal option and provide no opt-out instructions. However, at the end of their privacy policy is the following content.

"We are in compliance with the requirements of COPPA (Children's Online Privacy Protection Act), we do not collect any information from anyone under 13 years of age. Our website, products and services are all directed to people who are at least 13 years old or older."

COPPA is an act passed by congress in 1998 which can be found in its entirety online. It was created to place parents in control over what information is collected from their young children online. The Rule was designed to protect children under age 13 while accounting for the dynamic nature of the internet. The Rule applies to operators of commercial websites and online services directed to children under 13 that collect, use, or disclose personal information from children, and it applies to operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13. Basically, it makes it illegal for a website to knowingly display any personal information about children under the age of 13. This is one reason you see many social networks enforce an age limit.

You can use this to your advantage. If you have a child under the age of 13 in your home, this may be a way to force websites to remove your information. Let me explain by providing two different scenarios.

Scenario # 1: Your child is eight years of age and lives in your residence. You conducted a search of your cellular telephone number on cellrevealer.com which identified your name and address. On occasion, your child uses this telephone number to communicate with friends and family. Therefore, it is fair to say that cellrevealer.com currently displays information that identifies a cellular telephone number used by a child under the age of thirteen and associates the number with the child's home address.

Scenario # 2: You have no children, but you have a niece that is ten years of age that occasionally visits your house. When she is there, she often uses your landline telephone to stay in touch with her parents. You located your landline telephone number listed on numberguru.com which identified your home address. Therefore, it is fair to say that numberguru.com currently displays information that identifies a landline telephone number used by a child under the age of 13 and associates the number with the child's current location.

Sending the following email to any contact email address on the website should generate immediate action.

"It has come to my attention that your website displays information that identifies a cellular telephone number used by a child under the age of 13 and

associates the number with the child's home address. This is a violation of the Children's Online Privacy Protection Act (COPPA). I request that the following information be removed from your database immediately."

This probably sounds sneaky and misleading. Only you can decide if protecting your privacy is worth any ethical dilemmas. In my collective conscience it is more unethical to collect personal information from people and broadcast it to the world for a profit than to use legal loopholes to have your own information removed. This tactic could be applied to other websites that disclose information such as home addresses, social network data, personal interests, and friends or associates. In my experience, few companies will decline a request such as this. They are more afraid of being sued than eliminating a single entry.

Everything Else

By the time that you read these words, much will have changed in the world of digital privacy. I began documenting methods for information removal in 2011. It was much more manageable then and changes rarely occurred. Today, new data collection websites seem to appear daily and the existing sites change their removal process often. No written work like this can remain timeless in our digital age. This portion is designed to aid you with any future issues that you discover which jeopardize your right to privacy.

Privacy Policies

You will likely encounter new personal information websites that are not listed in this book. During your Pre-Assessment, you may find unique online information about yourself that you want removed. When an opt-out process is not obvious on the website, always look for a privacy policy page. These are often linked from the very bottom of the home page and the link is commonly in small print.

The privacy pages often contain very detailed text about how the company receives and shares the personal information that it collects. It will usually discuss how it uses cookies on your computer to collect further details and what your options are for disabling this technology. Many of the techniques that I

have shared in this book come directly from privacy pages of the businesses discussed. Look for specific instructions to opt-out or remove your information through these pages.

Some websites possess a privacy policy page but do not link to it from their home page. This fulfills the requirement to offer an opt-out process, but makes it difficult to locate the page with instructions. A specific query on Google or any other search engine should assist you. While researching everify.com, I immediately noticed that there was not an obvious opt-out process or privacy page, but eventually learned that these details were stored within a small "Legal" link between several other unrelated links. Instead of clicking through a lot of irrelevant content, you can conduct the following search on Google.

Site:everify.com "Opt-out"

In this example, "site:everify.com" instructs Google to only search one specific domain. It will ignore any other websites and bring all results relevant to your search. The "Opt-out" within quotation marks informs Google to only display results that have that exact phrase within the page or document. The actual result of this search is a PDF document that is exactly what you would need to complete their removal process. Still using everify.com as an example, the following searches may be helpful. Replace everify.com with the website name from which you are trying to remove your information.

Site:everify.com "privacy page"
Site:everify.com "privacy policy"
Site:everify.com "privacy"
Site:everify.com "opt out"
Site:everify.com "removal"
Site:everify.com "legal"

Email Messages

Some services will not offer an online form or document for personal information removal. They may force you to contact them directly with your request. For many companies, this fulfills their obligation to offer a removal

option. The direct contact deters many people from proceeding with the process. An email message will often achieve the desired result.

Identifying the appropriate email address to send requests can range from obvious to difficult. Many privacy policy pages include a generic account for opt-out requests such as privacy@ebureau.com. This is likely an account that is monitored by many different people. I list these in the workbook section as I find them. Some services do not publicly list the most appropriate address, so you will need to take a couple of additional steps in order to locate a helpful address.

Email Assumptions

Most companies have a standard format for all of their email addresses. This will often include a combination of a last name and first name at the business domain, such as john.smith@ebureau .com. These companies usually also have a standard account that is set up to receive requests for removal of information, such as privacy@ebureau.com. Any time you find a company that does not include an obvious removal process for your personal data, consider sending an email to several possible accounts. In the case of ebureau.com, you could send a removal request to the following accounts.

remove@ebureau.com
removal@ebureau.com
optout@ebureau.com
opt-out@ebureau.com
privacy@ebureau.com
legal@ebureau.com
info@ebureau.com
questions@ebureau.com
contact@ebureau.com
support@ebureau.com
admin@ebureau.com

Some of these email addresses will likely not exist and you will receive a message delivery error. Often, you will be fortunate in delivering at least one message to someone that can help. If you want to be more precise about this tactic, you could test the email addresses first.

Email Verification

Mail Tester (mailtester.com) is a free service that will allow you to immediately test an email address to determine if it is valid. The response will confirm that an email server exists, that it is functioning, and that the designated email address is real. A valid email result should be all green in color while any presence of red indicates a bad address.

LinkedIn

If you have submitted email messages to the standard accounts such as remove and privacy, and did not get any results, you may consider contacting key employees directly. The best way to identify the appropriate contacts is through LinkedIn (linkedin.com).

As an actual example, assume that you have completed the information removal process at EBureau, but your information was never removed. You now want to reach out to a real human for assistance. The following steps will likely receive a response from an employee.

- ✓ Conduct a search for “EBureau” on LinkedIn. Many of these will not display the name of the person, and will only display “LinkedIn Member”. Some will display the name of the employee.

- ✓ Attempt to identify an employee that possesses an important role at the company. My search displayed the profile of a senior vice president of EBureau. Unfortunately, the name is redacted, but you can still identify it with some internet investigation.

- ✓ Open the profile and right-click on the photo. Choose the option to copy the image location, which is sometimes referred to as the image URL.

- ✓ Connect to images.google.com and click on the small camera icon within the search field. This will display a new window. Paste the

URL or address of the LinkedIn image and click “Search by image”. It identifies another identical image which identifies the individual as Mic O’Brien.

- ✓ Alternatively, search Google for the terms “Vice President EBureau” and document any employee names discovered.

- ✓ Determine the email format of employee addresses at the company. Search for “@ebureau.com” with the quotation marks to identify any email addresses publicly visible. A search result identified a website announcing an EBureau event that includes contact information. These details announce that Anna Haire’s email address is annahaire@ebureau.com. We can now assume that the email format is first name + last name @ebureau.com.

- ✓ Combine the employee names that you discovered with the domain of @bureau.com and test them with mailtester.com. This will display a result confirming micobrien@ebureau.com is valid. You now have the email address of a senior vice president at the company.

- ✓ Repeat this process for numerous employees and send each a polite request for action in regards to your removal request.

Fax Requests

Many businesses will publish a facsimile (fax) number on their public websites. While these numbers may not be the appropriate reception for removal requests, the message will be received by an employee who may forward it to the person responsible for the information. Conduct the following steps in order to identify the fax numbers of a business.

Perform a Google search for the name of the company and the word fax, both within separate quotation marks. My search identified a valid fax number of 320-534-5020 for that business.

Direct Telephone Call

If all else fails to get you the results you desire, consider making a telephone call. This has been the least effective method in my experience. However, I have on occasion spoken to very helpful employees who were willing to help me and remove my information. Since most people do not choose this method, employees are fairly surprised to get a call for a removal request. Search through the target business' websites and conduct searches for the company name and the word "phone".

Additional Privacy Information

I learn new information about our privacy, and lack of, every day while I conduct research for my own purposes. One of the best resources for extremely current content is the Privacy page on Reddit. I encourage you to visit and bookmark the following website for the most vital information about the state of our privacy: reddit.com/r/Privacy.

Online Removal Databases

On the following pages, I have tried to identify the most common online databases that reveal personal details about you. I have found that removing information from these services has the most impact toward your overall online privacy. Listing every service that may have information stored about you is not feasible. Fortunately, there are several websites that maintain a list of removal options. You can always find a current list of Opt-Out instructions for most data vendors at the following websites.

www.inteltechniques.com
www.computercrimeinfo.com
www.justdelete.me
www.privacyrights.org/online-information-brokers-list
www.abine.com/optouts.php

While this book maintains a focus for removal from the most prevalent data collection companies, you may find your information on a smaller or unlisted

website. One of these sites will likely list the removal options and a direct link to a page to assist with the process.

It is now time for you to attack the invasive websites that disclose your private information to the world. Begin your adventure on the next page.

Service: **10 Digits** **Category**: Telephone Search
Website: 10digits.us
Removal Link: 10digits.us/remove
Privacy Policy: 10digits.us/privacy/
Email Address: mail@10digits.us
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **411** **Category**: Telephone Search
Website: 411.com
Removal Link: None
Privacy Policy: www.whitepagescustomers.com/data-policy/
Email Address: support@411.com, support@whitepages.com
Requirements: Online submission
Notes: Remove entry from whitepages.com
Date: _____
Response: _____
Verified Removal: _____

Service: **411 Info** **Category**: Telephone Search
Website: 411.info
Removal Link: 411.info/manage/
Privacy Policy: 411.info/privacy/
Email Address: support@411.info, admin@411.info
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **Addresses** **Category**: People Search
Website: addresses.com

Removal Link: addresses.com/optout.php
Privacy Policy: www.addresses.com/terms.php
Email Address: support@addresses.com, admin@addresses.com
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: Advanced Background Checks — Category: People Search

Website: advancedbackgroundchecks.com
Removal Link: advancedbackgroundchecks.com/optout-form.pdf
Privacy Policy: www.advancedbackgroundchecks.com/privacy
Email Address: Unknown
Requirements: Postal mail submission
Notes: Print and mail online form.
Date: _____
Response: _____
Verified Removal: _____

Service: Anywho — Category: People Search

Website: anywho.com
Removal Link: None
Privacy Policy: corporate.yp.com/privacy-policy/
Email Address: ypcsupport@yp.com, press@yp.com
Requirements: Online submission
Notes: Select profile and choose “Remove Listing”.
Date: _____
Response: _____
Verified Removal: _____

Service: DOB Search — Category: People Search

Website: www.dobsearch.com
Removal Link: Embedded into results
Privacy Policy: www.dobsearch.com/privacy.php
Email Address: support@dobsearch.com

Requirements: Online submission
Notes: Search your name and click “Manage my listings” at bottom. Follow instructions.
Date: _____
Response: _____
Verified Removal: _____

Service: **Email Finder** **Category**: People Search

Website: emailfinder.com
Removal Link: www.emailfinder.com/EFC.aspx?_act=Optout
Privacy Policy: www.emailfinder.com/privacypolicy.shtml
Email Address: Unknown
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **Free Phone Tracer** **Category**: Telephone Search

Website: www. freephonetracer.com
Removal Link: freephonetracer.com/FCPT.aspx?_act=Optout
Privacy Policy: freephonetracer.com/FCPT.aspx?_act=PrivacyPolicy
Email Address: privacy@freephonetracer.com
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **Infospace** **Category**: People Search

Website: infospace.com
Removal Link: infospace.intelius.com/optout.php
Privacy Policy: support.infospace.com/privacy
Email Address: support@infospace.com, info@infospace.com
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **Lookup** **Category**: People Search
Website: lookup.com
Removal Link: lookup.com/optout.php
Privacy Policy: www. lookup.com/privacy.php
Email Address: optout@lookup.com
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **Lookup Anyone** **Category**: People Search
Website: lookupanyone.com
Removal Link: None
Privacy Policy: www.lookupanyone.com/privacy-faq.php
Email Address: support@lookupanyone.com, info@lookupanyone.com
Requirements: Fax submission
Notes: Send your custom opt-out request form via fax to 425-974-6194
Date: _____
Response: _____
Verified Removal: _____

Service: **MyLife** **Category**: People Search
Website: www.mylife.com
Removal Link: None
Privacy Policy: www.mylife.com/privacy-policy/
Email Address: privacy@mylife.com
Requirements: Email submission
Notes: Send email with removal request.
Date: _____
Response: _____
Verified Removal: _____

Service: **PeekYou** **Category**: People Search
Website: peekyou.com
Removal Link: www.peekyou.com/about/contact/optout/
Privacy Policy: www.peekyou.com/privacy
Email Address: support@peekyou.com
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **PeepDB** **Category**: People Search
Website: peepdb.com
Removal Link: None
Privacy Policy: www.peepdb.com/privacy.html
Email Address: info@peepdb.com
Requirements: Online submission
Notes: Locate your info and click on the “Remove This Listing” at bottom of page.
Date: _____
Response: _____
Verified Removal: _____

Service: **People By Name** **Category**: People Search
Website: peoplebyname.com
Removal Link: www.peoplebyname.com/remove.php
Privacy Policy: www.peoplebyname.com/privacy.php
Email Address: support@peoplebyname.com
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **People Finder** **Category**: People Search
Website: peoplefinder.com
Removal Link: peoplefinder.com/optout.php
Privacy Policy: peoplefinder.com/privacy/

Email Address: support@peoplefinder.com, info@peoplefinder.com
Requirements: Online submission, email verification
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **People Finders** **Category**: People Search

Website: peoplefinders.com
Removal Link: peoplefinders.com/manage/default.aspx
Privacy Policy: www.peoplefinders.com/privacy.aspx
Email Address: support@peoplefinders.com
Requirements: Online submission, email verification
Notes: Select your profile, click “This is me”, then “Opt-out my info”.
Date: _____
Response: _____
Verified Removal: _____

Service: **People Lookup** **Category**: People Search

Website: peoplelookup.com
Removal Link: None
Privacy Policy: www.peoplelookup.com/privacy.php
Email Address: support@peoplelookup.com, info@peoplelookup.com
Requirements: Fax submission
Notes: Send your custom opt-out request form via fax to 425-974-6194
Date: _____
Response: _____
Verified Removal: _____

Service: **People Search Now** **Category**: People Search

Website: peoplesearchnow.com
Removal Link: www.peoplesearchnow.com/optout-form.pdf
Privacy Policy: www.peoplesearchnow.com/privacy
Email Address: support@peoplesearchnow.com, info@peoplesearchnow.com
Requirements: Postal mail submission
Notes: Complete form and mail to listed address.
Date: _____
Response: _____

Verified Removal: _____

Service: **People Smart** **Category**: People Search
Website: peoplesmart.com
Removal Link: www.peoplesmart.com/optout-go
Privacy Policy: www.peoplesmart.com/privacy-policy
Email Address: privacy@peoplesmart.com
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **Phone Detective** **Category**: Telephone Search
Website: phonedetective.com
Removal Link: www.phonedetective.com/PD.aspx?_act=OptOut
Privacy Policy: www.phonedetective.com/PD.aspx?_act=PrivacyPolicy
Email Address: privacy@phonedetective.com
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **Phone Number** **Category**: Telephone Search
Website: phonenumber.com
Removal Link: None
Privacy Policy: www.whitepagescustomers.com/data-policy/
Email Address: support@phonenumber.com, support@whitepages.com
Requirements: Online submission
Notes: Remove entry from whitepages.com
Date: _____
Response: _____
Verified Removal: _____

Service: **Pipl** **Category**: People Search
Website: pipl.com
Removal Link: pipl.com/directory/remove
Privacy Policy: pipl.com/privacy
Email Address: support@pipl.com, mail@pipl.com
Requirements: Online submission, email verification
Notes: Must enter the required URL with your name as explained on the page.
Date: _____
Response: _____
Verified Removal: _____

Service: **Poedit** **Category**: People Search
Website: poedit.org
Removal Link: toppeoplefinder.com/remove.aspx
Privacy Policy: toppeoplefinder.com/privacy.aspx
Email Address: Unknown
Requirements: Online submission
Notes: Select profile, copy URL, click “Removal Request” at bottom of page.
Date: _____
Response: _____
Verified Removal: _____

Service: **Public Records 360** **Category**: People Search
Website: publicrecords360.com
Removal Link: publicrecords360.com/optout.html
Privacy Policy: www.publicrecords360.com/privacy.html
Email Address: optout@publicrecords360.com, privacy@ publicrecords360.com
Requirements: Postal mail submission
Notes: Complete opt-out form and email with ID to optout@publicrecords360.com.
Date: _____
Response: _____
Verified Removal: _____

Service: **Radaris** **Category**: People Search
Website: radaris.com
Removal Link: None
Privacy Policy: radaris.com/page/privacy

Email Address: support@radaris.com, info@radaris.com
Requirements: Online submission, email verification
Notes: Select your profile; click “Information control” then “Hide Information”.
Date: _____
Response: _____
Verified Removal: _____

Service: **Reverse Genie** **Category**: People Search
Website: www.reversegenie.com
Removal Link: None
Privacy Policy: www.reversegenie.com/privacy.php
Email Address: support@reversegeniwe.com
Requirements: Postal mail or fax submission
Notes: Follow online instructions at www.reversegenie.com/data_optout.php
Date: _____
Response: _____
Verified Removal: _____

Service: **Reverse Phone Lookup** **Category**: Telephone Search
Website: www. reversephonelookup.com
Removal Link: reversephonelookup.com/remove.php
Privacy Policy: www.reversephonelookup.com/privacy.html
Email Address: support@reversephonelookup.com, info@reversephonelookup.com
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **Sales Spider** **Category**: Business Search
Website: salespider.com
Removal Link: None
Privacy Policy: www.salespider.com/index.php?privacy=1
Email Address: support@salespider.com
Requirements: Online submission
Notes: Locate profile and select “Delete this profile”.
Date: _____
Response: _____

Verified Removal: _____

Service: **Search Bug** **Category**: People Search
Website: www.searchbug.com/tools/reverse-phone-lookup.aspx
Removal Link: None
Privacy Policy: www.searchbug.com/privacy.aspx
Email Address: support@searchbug.com
Requirements: Online submission
Notes: Follow online instructions at www.searchbug.com/help.aspx?WHAT=people
Date: _____
Response: _____
Verified Removal: _____

Service: **Spokeo** **Category**: People Search
Website: spokeo.com
Removal Link: www.spokeo.com/optout
Privacy Policy: www.spokeo.com/privacy
Email Address: support@spokeo.com, customercare@spokeo.com
Requirements: Online submission, email verification
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **Super Pages** **Category**: Telephone Search
Website: www.superpages.com
Removal Link: None
Privacy Policy: www.superpages.com/about/privacy.html
Email Address: support@superpages.com, info@superpages.com
Requirements: Online submission
Notes: Select profile and choose “Remove Listing”.
Date: _____
Response: _____
Verified Removal: _____

Service: **SwitchBoard** **Category**: People Search
Website: switchboard.com
Removal Link: switchboard.intelius.com/optout.php
Privacy Policy: www.switchboard.com/privacy_central
Email Address: info@switchboard.com, support@switchboard.com
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **That's Them** **Category**: People Search
Website: thatsthem.com
Removal Link: thatsthem.com/optout
Privacy Policy: thatsthem.com/privacy
Email Address: Unknown
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **Top People Finder** **Category**: People Search
Website: toppeoplefinder.com
Removal Link: toppeoplefinder.com/remove.aspx
Privacy Policy: toppeoplefinder.com/privacy.aspx
Email Address: Unknown
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **US Identify** **Category**: People Search
Website: usidentify.com
Removal Link: None
Privacy Policy: www.usidentify.com/company/privacy.html

Email Address: privacy@peoplesmart.com
Requirements: Postal mail submission
Notes: Send custom opt-out form to address on privacy policy page.
Date: _____
Response: _____
Verified Removal: _____

Service: US Search **Category**: People Search

Website: ussearch.com
Removal Link: ussearch.com/privacylock
Privacy Policy: ussearch.com/about/privacy
Email Address: cservice@ussearch.com, social@ussearch.com
Requirements: Online submission and fax report
Notes: Online removal tool will generate form. Fax form to 425-974-6242.
Date: _____
Response: _____
Verified Removal: _____

Service: W9R **Category**: People Search

Website: w9r.com
Removal Link: None
Privacy Policy: www.w9r.com/about/privacy.html
Email Address: support@w9r.com
Requirements: Online submission
Notes: Locate profile and select “Opt out or remove”.
Date: _____
Response: _____
Verified Removal: _____

Service: White Pages **Category**: Telephone Search

Website: whitepages.com
Removal Link: None
Privacy Policy: **www.**whitepages.com/data-policy
Email Address: support@whitepages.com
Requirements: Online submission
Notes: Locate profile, click “Edit”, create anonymous account, delete as desired.
Date: _____
Response: _____

Verified Removal: _____

Service: **Yasni** **Category**: People Search

Website: yasni.com
Removal Link: None
Privacy Policy: yasni.com/privacy
Email Address: info@yasni.com, support@yasni.com
Requirements: Remove data from the original source
Notes: No removal option, but will identify sources of data. Will refresh occasionally.
Date: _____
Response: _____
Verified Removal: _____

Service: **Yellow Pages** **Category**: Telephone Search

Website: www.yellowpages.com/reversephonelookup
Removal Link: None
Privacy Policy: corporate.yp.com/privacy-policy/
Email Address: ypcsupport@yp.com, press@yp.com
Requirements: Online submission
Notes: Select profile and choose “Remove Listing”.
Date: _____
Response: _____
Verified Removal: _____

Service: **Zabasearch** **Category**: People Search

Website: zabasearch.com
Removal Link: None
Privacy Policy: zabasearch.com/privacy.php
Email Address: info@zabasearch.com, response@zabasearch.com
Requirements: Fax submission
Notes: Send your custom opt-out request form via fax to 425-974-6194.
Date: _____
Response: _____
Verified Removal: _____

Service: **ZoomInfo** **Category**: Business Info
Website: zoominfo.com
Removal Link: None
Privacy Policy: www.zoominfo.com/business/about-zoominfo/privacy-center
Email Address: info@zoominfo.com, support@zoominfo.com
Requirements: Online submission, email verification
Notes: Click “Is this you?” in your profile. Signup and delete desired details.
Date: _____
Response: _____
Verified Removal: _____

Public Data Brokers

Data brokers collect public information like names, home addresses, purchase histories, credit card activity and other sensitive data. They create large databases and then sell copies to other companies. It’s mostly marketing companies that are interested, particularly those that do online targeting. But most will sell the data to anyone that will pay. Some of the companies mentioned in the previous section are technically data brokers. Since their primary purpose is locating people, they were isolated from those in this section. The companies mentioned in this section collect and sell much more data about you.

Aside from the basics needed to locate you, these data brokers, sometimes called information brokers, go deeper into your life to build a profile on you. Their databases include your DMV records, property records, voter records, weapon permits, internet search history, online comments, online aliases, shopping history, court history, and much more. Most of this is also geo-coded, which provides your location when the information was gathered. This is all done thanks to the advancements in technology and the internet. These companies take this data and package it into a profile that can be easily analyzed and used to target more products and services toward you. Removing your information from these databases will be similar to the previous methods discussed earlier. Much like the previous section, these instructions are presented in workbook format. If anything ever seems unclear, refer to the privacy policy link. Consider the following tips.

- ✓ Never use your real email address. Use the new anonymous address that was created earlier. Most, if not all, of these services will allow

you to use your 33 Mail forwarding address.

- ✓ Only provide information to these services that they already know. If you find your name and address on one service, it is safe to assume that they all know it, but do not voluntarily provide it.

- ✓ For those that require a postal mail submission, be sure to include all documentation required per the privacy page listed for each service. If you fail to include any mandated information, they will deny your request. They are not required to notify you of this denial.

- ✓ Take notes as you work through this process. Use a pencil or photocopy these pages for additional future use.

Begin your removal of personal data from public data brokers on the next page.

Service: **Accutellus** **Category**: Public Data Broker
Website: accutellus.com
Removal Link: accutellus.com/opt_out_request.php
Privacy Policy: www.accutellus.com/terms.php
Email Address: Unknown
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **Address Search** **Category**: Public Data Broker
Website: adresssearch.com
Removal Link: addresssearch.com/remove-info.php
Privacy Policy: www.addresssearch.com/privacy-policy.php
Email Address: support@addresssearch.com
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **Axciom** **Category**: Public Data Broker
Website: www. acxiom.com
Removal Link: www.isapps.acxiom.com/optout/optout.aspx
Privacy Policy: www.acxiom.com/about-acxiom/privacy/us-products-privacy-policy/
Email Address: consumeradvo@acxiom.com
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **Been Verified** **Category**: Public Data Broker
Website: www.beenverified.com

Removal Link: www.beenverified.com/faq/opt-out/
Privacy Policy: www.beenverified.com/privacy
Email Address: privacy@beenverified.com
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **Complete Investigation Services** **Category**: Public Data Broker
Website: www.cisnationwide.com
Removal Link: cisnationwide.com/optout.html
Privacy Policy: cisnationwide.com/privacy.html
Email Address: support@cisnationwide.com
Requirements: Fax submission
Notes: Fax required documents to 888-446-1229.
Date: _____
Response: _____
Verified Removal: _____

Service: **Confi-Chek** **Category** : Public Data Broker
Website: confi-chek.com
Removal Link: None
Privacy Policy: None
Email Address: support@confi-chek.com
Requirements: Postal mail submission
Notes: Send opt-out form to PO Box 110850, Naples, Florida 34108.
Date: _____
Response: _____
Verified Removal: _____

Service: **Core Logic** **Category**: Public Data Broker
Website: www.corelogic.com
Removal Link: None
Privacy Policy: www.corelogic.com/privacy.aspx
Email Address: privacy@ebureau.com

Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **Data Detective** **Category**: Public Data Broker
Website: datadetective.com
Removal Link: www.datalogix.com/privacy/#opt-out-landing
Privacy Policy: www.datalogix.com/privacy/
Email Address: Unknown
Requirements: Fax submission
Notes: Fax required documents under “Opt Out Policy” to 617-993-9946.
Date: _____
Response: _____
Verified Removal: _____

Service: **Datalogix** **Category**: Public Data Broker
Website: datalogix.com
Removal Link: None
Privacy Policy: www.interactivedata.com/privacy-policy/
Email Address: support@datalogix.com
Requirements: Online submission
Notes: Follow instructions under “Choice” section of removal link.
Date: _____
Response: _____
Verified Removal: _____

Service: **EBureau** **Category**: Public Data Broker
Website: ebureau.com
Removal Link: www.ebureau.com/privacy-center/opt-out
Privacy Policy: www.ebureau.com/privacy-center
Email Address: Unknown
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **Instant Check Mate** **Category**: Public Data Broker
Website: instantcheckmate.com
Removal Link: instantcheckmate.com/optout
Privacy Policy: www.instantcheckmate.com/privacy_policy/
Email Address: privacy@instantcheckmate.com, support@instantcheckmate.com
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **Intelius** **Category**: Public Data Broker
Website: intelius.com
Removal Link: www.intelius.com/optout.php
Privacy Policy: www.intelius.com/privacy.php
Email Address: privacy@intelius.com
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **Interactive Data** **Category**: Public Data Broker
Website: interactivedata.com
Removal Link: None
Privacy Policy: www.interactivedata.com/privacy-policy/
Email Address: Investor.Relations@interactivedata.com
Requirements: Postal mail submission
Notes: Send opt-out form to address on privacy page.
Date: _____
Response: _____
Verified Removal: _____

Service: **LexisNexis Direct Marketing** **Category**: Public Data Broker

Website: www.lexisnexis.com
Removal Link: www.lexisnexis.com/privacy/directmarketingopt-out.aspx
Privacy Policy: www.lexisnexis.com/privacy/
Email Address: privacy.information.mgr@lexisnexis.com
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **LexisNexis People Locator** **Category**: Public Data Broker

Website: phonedetective.com
Removal Link: None
Privacy Policy: www.lexisnexis.com/privacy/
Email Address: remove@prod.lexisnexis.com
Requirements: Postal mail submission
Notes: Follow instructions at lexis-nexis.com/clients/iip/removingInfo.htm
Date: _____
Response: _____
Verified Removal: _____

Service: **Tower Data** **Category**: Public Data Broker

Website: www. towerdata.com
Removal Link: dashboard.towerdata.com/optout/
Privacy Policy: www.towerdata.com/company/privacy_policy
Email Address: privacy@towerdata.com
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Non-Public Data Brokers

In Chapter Three, you created a general opt-out request form for submission to companies. A second form, the “extended form”, was mentioned which would include additional information that would qualify you to have further data removed. This data is often called non-public data. Such data is often shared with both government and private agencies. None of the methods in this chapter will prevent law enforcement from seeing your records. However, the techniques will help prevent your data from leaking into databases that can be bought by banks, lawyers, medical organizations, and credit agencies. I believe it is only a matter of time before these databases are breached and shared publicly.

These methods are not for everyone and the removal process is much stricter. The companies that sell this data allow people to have their information removed only if certain criteria are met. While each company offers specific wording on the requirements, the basic idea is that a person must fit into one of the following circumstances:

- ✓ The person is a judge, public official, or member of law enforcement in danger
- ✓ The person is the victim of aggravated identity theft
- ✓ The person is at risk of immediate physical harm

At first glance, you may think that you would not meet these requirements. The criteria are actually quite broad and many people can honestly declare that they fit into one of these statements. The first category is the most defined.

Judges: If you are a documented judge on a local, state, or federal level, you definitely meet the requirement. This also includes retired judges.

Public Officials: Many city, county, state, and federal employees are “public officials”. There is a good chance that whatever your duties are, you have a presence in the public. Elected officials or those that provide information to the public are the easiest to declare. If your position has ever required you to speak to the press, disclose information to the public, or respond to public inquires, you are a public official. It will ultimately be up to you to determine if you meet this

definition.

Law Enforcement: A substantial portion of this book's audience is law enforcement. Whether you are a part-time or full-time officer or agent, as long as you are sworn by your local agency, county, or state, you fit in this category. This also includes retired officers and agents. Recently, many companies have added a requirement that the person making the request be in a position of "immediate danger". Personally, I believe every law enforcement officer is in immediate danger. These companies may not have that opinion. I will provide optimal wording for your request in just a moment.

Aggravated Identity Theft: With the number of identity theft cases on the rise every year, more of you are now technically victims of this crime. Some of these cases are much worse than others. People that have had homes and vehicles purchased illegally in their names by criminals are obviously victims of identity theft. The FTC defines identity theft as a serious crime that "occurs when your personal information is stolen and used without your knowledge to commit fraud or other crimes".

Have you ever received a telephone call from your credit card company notifying you that someone is using your name and credit card number for unauthorized purchases? Have your friends told you that they received an email from your account telling them that you are stuck in another country and need money to get home? Has a disowned relative tried to open a credit line in your name to feed a drug habit? The examples are endless, but they all involve a situation where someone's "personal information is stolen and used without your knowledge to commit fraud or other crimes".

For some of these services, identity theft alone is not enough to qualify for removal. You must be the victim of aggravated identity theft, which is an enhanced form of identity theft. It occurs when someone knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person in the commission of particular felony violations. Basically, this occurs when someone uses false identification to commit identity theft against you. When this happens, you may never know about it. Therefore, I believe it is plausible that someone might be using identification in your name. I will discuss that further in a moment.

Ultimately, you must determine if you fit into this category. If you are ever the victim of identity theft, report it to your local police, and obtain a copy of the report. Most data companies require proof. In my experience, local police departments that take a report of identity theft from a citizen rarely follow-up on the complaint. The offender is likely from another state or another country where they have no jurisdiction.

Physical Harm: A person at risk of physical harm is allowed to have information removed from public access. I believe an argument could be made that any person is at risk of physical harm, but these companies do have some guidelines. Most want proof of this claim in the form of a police report identifying you as the victim of a violent crime or a copy of an order of protection issued by a court. Domestic abuse victims should have no problem meeting this requirement.

If you believe that you meet any of the criteria, you should create an extended opt-out request form. Basically, this is all of the information included on the basic form created in Chapter Three, but with a new section identifying how you meet one of the requirements. The data company may respond with a denial of your request, but this will not harm anything in your report. Many people have reported that sending a duplicate request after receiving a letter of denial resulted in a successful removal. Most likely, the person fielding requests is an entry level employee with little experience or authority in handling requests that vary from the norm.

To create the extended opt-out request form, open the basic opt-out request form that you created in Chapter Three. Remove the information that allowed for the entry of a URL of data found online. That will not be needed for these requests. In place of this section, you need to supply exactly how you fit into one of the qualifications mentioned earlier.

If you are a member of law enforcement, you could add a paragraph above your driver's license that states the following:

"I am a full-time sworn police officer in the state of _____ that is actively conducting investigations of violent subjects. This assignment has put me in immediate danger of physical harm. The attached letter from my supervisor

confirms my position and assignment."

If you are the victim of domestic abuse, sentences similar to the following could be added:

"I am a victim of domestic violence that has been reported to the police and prosecuted by the courts. I continue to fear for my safety. I have attached a copy of a police report/ order of protection for verification."

If you are a public official, maybe a parking enforcement employee for the city you live in, you could state the following:

"I am a full time parking enforcement official for the city of _____. This work as a public official has created a hostile working environment and I am often targeted by the public. The attached letter from my supervisor verifies my employment and assignment." If you are the victim of aggravated identity theft, sentences similar to the following could be added:

"I am the victim of aggravated identity theft. I have enclosed a police report filed in reference to this incident. It is believed that the offender(s) in this incident are representing themselves as me and likely possess identification in my name."

Including a police report verifying your claim is extremely helpful. This may not be feasible for you. I have had mixed success when including an affidavit signed by the victim. Many people believe an affidavit is something only created by law enforcement as part of a criminal trial. Anyone can create an affidavit. It is simply a written statement voluntarily made by a person under an oath or affirmation administered by a person authorized to do so by law. A notary public can declare your signature on an affidavit as authentic.

I recently had a client that was being harassed by an ex-boyfriend. The moment that she changed her telephone number, he would call her on it. After she moved to a new apartment, he showed up outside her door. He sent her borderline threats to every email address she possessed and created several social network profiles in her name containing slanderous comments. The local police could not identify a specific crime within his harassment that would qualify for

authorization of state charges. Instead, she created an affidavit. It read similar to the following.

“I am currently the victim of daily stalking by a former boyfriend. I have contacted the police. An investigation has been initiated. I have been threatened via various forms of communication including in-person, telephone, and electronic mail. The suspect in this incident has created an environment where I physically do not feel safe. I suspect that he is accessing information about me through non-public databases. These details have likely aided him in his attacks toward me.”

This affidavit was printed and signed in front of a notary public. The notary confirmed the signature and stamped the document with a state issued seal. This was enough to proceed with a data removal request. The request was authorized and a removal confirmation letter was received within weeks. Your mileage may vary with this technique. The worst case scenario is that your request is denied.

You need to create a statement that is accurate for your situation. Be prepared to verify this claim through a police report, affidavit, or letter from your supervisor. Only you can determine if you are eligible for the removal of your private information. I have a couple of thoughts about the ethics of these submissions.

First, do not be shy about the validity of your request. If you believe that you qualify for the removal of this extended non-public information, give it a shot. Remember, the worst that can happen is that your request is denied. These companies are not government entities. They will not prosecute you if they do not agree with your opinion of qualifying circumstances.

Next, persistence is your friend. If you are denied a request, resubmit the next day. It is highly unlikely that the same employee will receive the second request. However, it is likely that your profile will be notated during your previous removal denial. All you need is one sympathetic (or lazy) employee to approve the removal.

Hopefully, you are now ready to proceed with the removal requests for non-public data brokers. Use the following information to complete your requests.

Service: **Infopay/EVerify** **Category**: Non-Public Data Broker
Website: everify.com
Removal Link: www.everify.com/opt_out_form.pdf
Privacy Policy: www.everify.com/legal.php
Email Address: privacy@cisnationwide.com
Requirements: Postal mail or fax submission
Notes: Print form, complete, and mail to listed address or fax to 888-446-1229.
Date: _____
Response: _____
Verified Removal: _____

Service: **LexisNexis/Accurint** **Category**: Non-Public Data Broker
Website: lexisnexis.com
Removal Link: lexisnexis.com/opt-out-public-facing-products
Privacy Policy: www.lexisnexis.com/en-us/terms/privacy-policy.page
Email Address: privacy.information.mgr@lexisnexis.com
Requirements: Online submission
Notes: Online removal tool will complete the process. You can upload digital documents.
Date: _____
Response: _____
Verified Removal: _____

Service: **TLO** **Category**: Non-Public Data Broker
Website: tlo.com
Removal Link: None
Privacy Policy: www.tlo.com/privacy.html
Email Address: CustomerSupport@TLO.com, TLOxp@transunion.com
Requirements: Email submission
Notes: Send completed extended opt-out form and documentation to both email addresses.
Date: _____
Response: _____
Verified Removal: _____

Service: **Westlaw** **Category**: Non-Public Data Broker
Website: www. thomsonreuters.com

Removal Link: static.legalsolutions.thomsonreuters.com/static/pdf/opt_out_form.pdf
Privacy Policy: thomsonreuters.com/en/privacy-statement.html
Email Address: westlaw.privacypolicy@thomsonreuters.com
Requirements: Postal mail submission
Notes: Print form, complete, and mail to listed address. Include extended opt-out form.
Date: _____
Response: _____
Verified Removal: _____

Data Marketers

Data marketing companies sell personal data to businesses that want to sell a product or service. They collect information about you that assists them with matching these businesses to the most appropriate audience. These businesses include a wide range of organizations that sell everything from soda to mansions. The goal of data marketing companies is to identify people that are most likely to buy the specific product or service that a business is selling. When they do, they profit from this information and continue to build databases of your interests.

These marketing databases are less likely to be viewed by the general public than the databases discussed so far. Instead, they are bought, sold, and traded by private organizations that want to determine exactly how to entice you to buy something. You probably experience the effects of this every day.

For example, if you have a vehicle made in 2007, you will start to receive extended warranty options on that type of vehicle in the mail in 2012. Your name, address, phone number, and vehicle information is in a database sold to companies that provide vehicle warranty services. The package is purposely meant to look like an official manufacture warranty, and the intent is to make you believe that you should buy this warranty in order to keep your vehicle protected. Instead, these warranties are often provided by companies that will be difficult to contact when needed.

If you are shopping on the internet and researching a specific pair of shoes, your computer stores data that identifies your shopping history. This information is passed to other websites that you visit. You may start to see shoes similar to

those that you were looking at earlier begin to appear in advertisements on various pages as you browse the web. The goal of these ads is to determine what you are most likely to buy, and forward you to a website that will pay a premium for this information.

These are just two examples of the many ways that marketing companies try to keep track of what you are doing. It is common for companies such as these to have a complete profile on you that reveals more about your interests and buying habits than your closest friends and family are aware of. Similar to the earlier example of a department store knowing that a minor was pregnant before the family knew, businesses such as Amazon and Proctor & Gamble are using data to sell you more products.

If you enjoy receiving mailed advertisements, telephone calls, and emails encouraging you to buy specific products, you should skip this section. If you feel that this is an invasion into your privacy and are tired of being targeted for a profit, this should help.

DMA Choice

DMA Choice is an online tool located at dmachoice.org developed by the Direct Marketing Association to help you manage your postal mail and email advertisements. DMA Choice represents about 80% of the total volume of marketing mail in the United States. This website allows you to create an account and specify what types of mailing databases you want to be included in. Further, it allows you to specify if you want to be removed from an individual company's list or all of the different company's lists. To do this, you must create a free account which requires you to provide your name, home address and a valid email account. You must then identify individual companies that have your information and request removal from their databases. Another option is to request removal by category such as catalogs, magazines, donation requests, political mailings, and credit offers. This process is time consuming and still allows companies to collect your data if you had any type of relationship in the past.

There is an alternative solution. DMA Choice has two rarely used options that will remove a person's information out of the databases of all companies

associated with DMA Choice. It will also remove personal information from companies that have an existing relationship with the person requesting the removal. This could include credit companies that you have had a loan with in the past or retail stores where you had previously subscribed to a mailing list. These databases are referred to as their "Deceased Do Not Contact List" and "Do Not Contact for Caregivers List". Since I do not want to encourage people to fake their own death, you should use the caregiver's list option.

- ✓ Navigate to www.ims-dm.com/cgi/dncc.php and complete the online form. In the "Primary Name" section, provide your name and address only. If you receive mailings under another version of your name, such as Michael or Mike, add that name as well.

- ✓ In the "Information About You" section, you must provide the name of your "caregiver". Most likely, you do not have an official caregiver, but you do not need one for this unofficial request. I recommend that you provide the name of your mother or father. After all, they were your legal guardian while you were a child. If your parent is still living, he or she probably provides care to you in some form on occasion. If your parents are deceased, you can still put their name on this form. There is no verification process. Provide your anonymous email address where appropriate.

- ✓ Under the name of your "caregiver", there are five questions you must answer as your caregiver would answer. These are formalities of DMA Choice, and will not be verified. Only one question needs to have an answer of "Yes" to meet the minimum qualification.

Catalog Choice

If you find yourself bombarded with unwanted catalogs and advertisements in your mailbox, you are probably on many marketing lists as a valued shopper. The following instructions can be used to eliminate these mailings and remove your information from their databases. You must cancel with each individual company, but Catalog Choice makes this easy to do from one interface. If you do not receive unwanted catalogs, there is no need to complete these steps.

- ✓ Navigate to catalogchoice.org and click “Sign Up Now”. Supply your initials instead of your name, a password, and your anonymous email address. Be sure to un-check the option to receive email from them.

- ✓ On the next page, assign a nickname to your home address. This could be “Home”. Leave the “Company Name” blank and add your actual home address. Click “Save new address” when finished.

- ✓ You will receive an email from Catalog Choice. Open this message and click on the link inside the email. This will confirm your anonymous email address as active.

- ✓ When you receive unwanted mailings, log into this site and select “Find Companies”. Search for the company name and view the removal options. Usually, you will only need to click the “Submit Request” button at the bottom. This will send a notification to the desired company to remove you from all distributions.

- ✓ Since most companies remove the entry by address, your name is never required. If the company does require a name, they will see your initials that match the initials of the name that is in your profile. This will satisfy the requirements of the company removing you from their database.

I have used this successfully on several occasions. It usually works better than contacting the company directly. You do not need to submit a reason for removal; the default option is “Prefer not to answer”. The following section can be used as a workbook for eliminating your personal details from various data marketers. Many marketers can be avoided by simply using a secure web browser with privacy extensions as discussed in Chapter Four.

Service: **Catalog Choice** **Category**: Data Marketers
Website: catalogchoice.org
Removal Link: None
Privacy Policy: www.catalogchoice.org/privacy
Email Address: support@catalogchoice.org
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **DirectMail** **Category**: Data Marketers
Website: directmail.com
Removal Link: directmail.com/directory/mail_preference/
Privacy Policy: www.directmail.com/privacypolicy/
Email Address: donotmaillist@directmail.com
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **DMA Choice** **Category**: Data Marketers
Website: dmachoice.org
Removal Link: www.ims-dm.com/cgi/dncc.php
Privacy Policy: www.dmachoice.org/static/privacy_policy.php
Email Address: ethics@the-dma.org
Requirements: Online submission
Notes: Follow instructions on removal link.
Date: _____
Response: _____
Verified Removal: _____

Service: **Epsilon-Main** **Category**: Data Marketers
Website: epsilon.com

Removal Link: None
Privacy Policy: www.epsilon.com/privacy-policy/
Email Address: optout@epsilon.com
Requirements: Email submission
Notes: Send email with “Removal” as the subject. Include name and address.
Date: _____
Response: _____
Verified Removal: _____

Service: Epsilon-Abacus **Category**: Data Marketers

Website: epsilon.com
Removal Link: None
Privacy Policy: www.epsilon.com/privacy-policy/
Email Address: abacusoptout@epsilon.com
Requirements: Email submission
Notes: Send email with “Removal” as the subject. Include name and address.
Date: _____
Response: _____
Verified Removal: _____

Service: Epsilon-CFD **Category**: Data Marketers

Website: epsilon.com
Removal Link: None
Privacy Policy: www.epsilon.com/privacy-policy/
Email Address: dataoptout1@epsilon.com
Requirements: Email submission
Notes: Send email with “Removal” as the subject. Include name and address.
Date: _____
Response: _____
Verified Removal: _____

Service: Epsilon-Shopper **Category**: Data Marketers

Website: epsilon.com
Removal Link: None
Privacy Policy: www.epsilon.com/privacy-policy/
Email Address: contactus@shoppers-voice.com
Requirements: Email submission
Notes: Send email with “Removal” as the subject. Include name and address.

Date: _____
Response: _____
Verified Removal: _____

Service: **Haines & Company** **Category**: Data Marketers

Website: haines.com
Removal Link: None
Privacy Policy: None
Email Address: criscros@haines.com, info@haines.com, custserv@haines.com
Requirements: Email submission
Notes: Send email with name and address and request to be removed from all databases.
Date: _____
Response: _____
Verified Removal: _____

Service: **Infogroup** **Category**: Data Marketers

Website: infogroup.com
Removal Link: None
Privacy Policy: www.infogroup.com/privacy-policy
Email Address: contentfeedback@infogroup.com
Requirements: Email submission
Notes: Send email with “Opt-Out” as the subject. Include name and address.
Date: _____
Response: _____
Verified Removal: _____

Service: **Publishers Clearing House** **Category**: Data Marketers

Website: pch.com
Removal Link: None
Privacy Policy: www.pch.com/privacypolicy
Email Address: privacychoices@pchmail.com
Requirements: Email submission
Notes: Send email with name and address and request to be removed from all databases.
Date: _____
Response: _____
Verified Removal: _____

Service: **Vallasis/RedPlum-Main** **Category**: Data Marketers
Website: redplum.com
Removal Link: redplum.com/tools/redplum-postal-addremove.html
Privacy Policy: www.redplum.com/info/privacy
Email Address: wecare@vallasis.com
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **Valpak/ Cox** **Category**: Data Marketers
Website: Valpak.com
Removal Link: www.coxtarget.com/mailsuppression/s/DisplayMailSuppressionForm
Privacy Policy: www.coxtarget.com/privacy_policy.html
Email Address: legal@coxtarget.com
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Ancestry Records

I believe that online ancestry records are often overlooked by privacy enthusiasts. These family history websites seem innocent and educational on the surface. However, many of them expose details about you that should not be in public view. This often includes your full name, date of birth, address, and complete family history. Many of these services are available only to paying members, but removing your data is free. The following details should help you eliminate any unwanted information.

Service: **Ancestry** **Category**: Ancestry Search
Website: ancestry.com

Removal Link: None
Privacy Policy: www.ancestry.com/cs/legal/privacystatement
Email Address: support@ancestry.com, customersolutions@ancestry.com
Requirements: Email submission
Notes: Send message to both email addresses requesting specific information removal.
Date: _____
Response: _____
Verified Removal: _____

Service: **Archives** **Category**: Ancestry Search
Website: archives.com
Removal Link: archives.com/?_act=Optout
Privacy Policy: www.archives.com/privacy
Email Address: privacy@archives.com
Requirements: Online submission
Notes: Online removal tool will complete the process.
Date: _____
Response: _____
Verified Removal: _____

Service: **Family Search** **Category**: Ancestry Search
Website: familysearch.org
Removal Link: None
Privacy Policy: familysearch.org/privacy/
Email Address: DataPrivacyOfficer@ldschurch.org
Requirements: Email submission
Notes: Send message to email address requesting specific information removal.
Date: _____
Response: _____
Verified Removal: _____

Offensive Mailings

The United States Postal Service (USPS) offers a rarely used form to prohibit specific types of mailings from being delivered to your home. It is called a prohibitory order and was created to prevent adult content from reaching an audience of children. The Prohibitory Order program provides a deterrent to

continued mailings by a specific mailer advertising a product or service you consider erotically arousing or sexually provocative. Submitting this order will cause the USPS to demand the removal of your information from the database of the company that mailed the content. It is up to you to determine if content is arousing or provocative, and the power of this form should not be abused.

This method is targeted toward those with children. Police officers have used this technique to eliminate unwanted erotic mailings initiated by vengeful suspects. Families have used the form to stop adult content requested by mischievous friends of their children. Once any adult content is received at a home, it is very likely that the address will be added to several other adult content databases for future mailings. This form will also add the address to a database of addresses not wishing to receive adult advertisements.

- ✓ Navigate to about.usps.com/forms/ps1500.pdf and print the form. Complete all requested information and attach the original mailing that you find inappropriate. Deliver the form and offensive mailing to any post office.

Online Coupons

Many companies are embracing the idea of online coupons. These coupons can be printed from the internet and redeemed in stores like any other printed coupon. These appear to be very beneficial for the consumer. A person can conduct a brief search on various coupon websites for a specific product. When a coupon is located, it can be printed and applied to the sale of the product. Unfortunately, many people are not aware of what is happening behind the scenes with most online coupons.

Most of today's online coupons use special bar codes that help identify information about the life of the coupon. Each of these online coupons has a unique serial number embedded into the bar code. This can allow a company to track the date and time it was obtained, viewed, and redeemed. It can also identify the store where it was used and the original search terms typed to find it. This is all reported back to the original source of the digital coupon. Retailers are combining this data with information discovered online and off, such as your age, sex, income, shopping history, internet history, and your current location or

geographic routine. This creates a profile of the customer that is more detailed than ever. This profile can also include the other products purchased during the transaction and form of payment.

If you choose to use printable coupons, you have no choice but to give up some privacy. Here are some suggestions if you want to continue receiving these deals.

- ✓ When prompted for personal information, supply an alternate name. These details are seldom verified by the coupon delivery system.

- ✓ Log out of any social networks, especially Facebook, while researching and printing coupons. Companies will collect your profile data to associate you with the coupon and purchase history.

Loyalty and Reward Cards

Large stores such as Safeway and Vons offer a loyalty card, sometimes referred to as a reward card, to shoppers for instant savings on products. These stores offer “members only” sales that discount specific products for customers that have a membership card. If a customer does not have a card, the full price is charged instead of the sale price. This business model encourages a customer to favor a specific business for discounted items. Further, the business now possesses a large pool of information about customers.

Since customers are required to disclose their name, address, phone number, date of birth, gender, and email address to receive a card, stores can create an individual profile of your habits. This profile can include the items you buy, dates and times of purchases, form of payment, and location of purchase. They can also analyze the data and determine how often you buy a product, the amount you will spend on a product, and your overall value to the business. This data helps them individually target you with advertisements and track your redemption. The data can then be shared with other companies, law enforcement, private investigators, attorneys, and anyone else that will pay or use the courts to obtain the data.

I still encourage people to use these cards. In a later chapter, I will explain how

these programs can be beneficial for the purposes of disinformation. I provide the following suggestions when using any type of rewards or loyalty program that relies on physical cards to redeem savings:

- ✓ Immediately stop using your current loyalty cards. Apply for a new card as needed at the customer service area of the store.

- ✓ Provide an alternate name on the application for the card. Provide a real mailing address, but not yours. The address should exist. I recommend supplying the address of the store that you are requesting the membership. If the store requires you show identification, tell them that you just moved and the address on your license is inaccurate.

- ✓ Most loyalty cards insist on a working telephone number. This number can be used to access your account in case you lose your card. Provide your anonymous telephone number created in Chapter Three.

- ✓ Trade your loyalty cards with other people whenever you get the chance. Explain the privacy concerns to friends and family and encourage them to swap cards with you. I have not found success in approaching strangers with this method. It tends to generate skepticism and a complaint to the store manager.

These techniques will stop a large portion of the marketing projected toward you. None of these methods will remove your information from every marketing database. There will still be occasional evidence of your details being sold to another company. A later chapter will identify methods to notify you if this happens.

Summary

Removing your personal details from online databases is a huge step toward both privacy and security. The absence of the online information will help keep your home address and telephone number private. The absence of this data within

stored and traded databases will keep you more secure. The next time the data is compromised, you will not be present in it.

I recommend revisiting this chapter yearly. After removal the first time, it should not take you long to search for any newly populated details. No written work can provide information about every data collection company. However, this should give you a great starting point. Removing data from these sources will have a trickle effect. Smaller companies that purchase and broadcast this information will not have your details. Please visit my blogs and subscribe to my newsletter for constant updates about new sources.

Chapter Nine

Social Networks

With the explosion of social networks, many data mining companies are now collecting content from public profiles and adding it to a person's record. Overall, society has made it acceptable to provide every level of personal detail to the corporations that own these networks. We have been trained to "like" or "favorite" anything that we find enjoyable or feel pressured into identifying with. These actions seem innocent until we discover the extent of usage of this data. Think about your online actions another way. Would you ever consider spending time every day submitting personal details to online survey websites? Further, would you consider doing this for free?

Essentially, when you create a Facebook account you are agreeing to work as unpaid survey-taker, photographer, and writer. When you "like" a site you are adding to Facebook's trove of data about you. When you install the Facebook app on your phone you often give Facebook permission to access your location data, letting the service track you everywhere you go. When you upload photos to Instagram you are actually giving them, in perpetuity, to Facebook who can use them for almost any purpose whatsoever. When you update your status, submit a photo, or comment on Facebook you are voluntarily giving them data they can resell or reuse in almost any legal way. This is in addition to the fact that all your posts, status updates, likes, and other actions are used to build an incredibly accurate profile about you. Your photos are used in facial recognition software so accurately that Facebook could conceivably build a near-perfect 3D model of your body. Facebook exemplifies the axiom that if a product is free, you aren't the customer. You are the product.

The other danger of social networks and other services that rely on data collection is that they never forget. While you can delete your Facebook or

Google account, the information that you have submitted to the service will always be retained in some form. While Google may not keep the entirety of your emails, your profile will be saved for potential future use. While using some of these services, teenagers and adults are making irreversible decisions.

Before you learn how to remove your social network data from the companies that sell it, you must first clean up your social network profiles. Otherwise, the data companies will eventually collect the data from your profile and create a new database on you. The level of difficulty with the privacy strategies will depend on how much information you have already made available.

There are hundreds of social networks. The largest networks will be discussed in this chapter. You should visit any social network where you have created a profile. Even if you think that there was no personal information provided, take a look at both the public page visible to anyone on the internet and the “private” page visible only to friends. Evaluate the information that could be gathered about you and then log into the social network and see what information was provided when you created the account. Make note of all of this and consider the next three topics.

Privacy Settings

Most social networks provide an option to protect your personal details from the public. This is usually in the form of privacy settings that you can customize. These settings allow you to specify who can see the content of your profile. This can determine who can see your messages, photos, current location, employer and alumni information, friends and family, and other details. You can specify that either the public can see everything, or that certain details can only be viewed by people that you have classified as “friends”. Facebook also provides another option of “Friends of friends”. This means that people that you do not know can see your information if they know someone that you have classified as a friend. Modifying these settings to restrict who can see your data is advised. But, it can also create a false sense of security and encourage you to post sensitive content. Here are a few of things to consider about privacy settings.

These settings only prohibit the public from seeing the content. The content is still visible to the company that owns the social network. When you created the

account, you agreed to a long list of legal terms called the terms of service. These terms probably discussed how the company that owns the social network can do whatever they want with the data that you provide. While these networks may be careful not to share your private data now, no one knows what will happen in the future.

Privacy settings can also be incredibly confusing. Some larger social networks may have dozens of privacy settings and hundreds of combinations of settings. This can make choosing the most private and secure options difficult. Privacy settings are subject to change. Facebook is notorious for updating its privacy policy to allow more and more of your data to become less and less private. Frequently, when the privacy policy changes many of your privacy settings will change. When these automatic changes occur, they will not be in the interest of privacy. They will be to the benefit of the social network and will make as much of your information public and accessible as possible.

It is common to read in technology news sources about people that break into other people's accounts to steal information. Celebrities are continually having their accounts compromised by self-proclaimed "hackers" for both fun and profit. If someone wants your data bad enough, and has the money to fund an expedition to retrieve your data, there is a criminal ready to complete the task.

Finally, there are many legal ways to retrieve data that is believed to be private. I have demonstrated during my law enforcement training how videos and photos from "hidden" MySpace profiles can be located through Google and how the Twitter API can reveal personal details that are not visible on a person's profile page including exact location. Many people take a quick glance at their profile and are satisfied that only those with approved access can see their content. They are often wrong.

I believe that any time you post anything to the internet you must assume it is for public view. Even if you have your privacy settings locked as tight as possible, you should accept that there is a possibility that someone else could get your data. If the content you are uploading to your private page would also be acceptable for public view, then you can proceed. However, if the photos of you drunk the night before would embarrass you if anyone but your friends saw it, you should not take the chance. Privacy settings will not always save you.

Content Removal

If you have looked at your profiles and have identified personal data that you no longer want on the internet, you can remove it. There are too many different social networks to provide instruction for the removal of specific information. The process is usually fairly easy. If you have trouble, conduct an internet search for the answers. Ultimately, any information that you provided to your profile can be removed. The exception may be your name on certain sites. If you find something that you cannot remove, choose to update the information and insert blank spaces or disinformation.

Most likely, it will not be your profile that contains information that worries you. It will probably be the profiles of your children and other relatives. Many teenaged children have no concern about privacy and the dangers of online information. Many will post hundreds of photos from their daily habits that will expose every intimate detail of their lives. There is nothing legal that you can do to modify this information on your own. Often, a calm yet stern talk with your children will start the process of cleaning up the profiles.

Delete Accounts

By now, you may be considering completely removing all of your social networks. This process is not as easy as you would think. Social networks want your profiles, and more importantly your eyes on their advertisements. Facebook's home page does not inform you how to delete your account. Actually, no social network does this. It is very important to delete your accounts in a specific manner to ensure that the data is removed. The process to do this on several popular networks will be explained here.

Facebook (facebook.com)

If your Facebook content is public, there are several data mining sites collecting everything that you post including comments, photos, and friends. The first layer of privacy that you should implement is appropriate privacy settings. Recently, Facebook made this process much easier than before. After you login to your account, click on the "down arrow" in the upper right corner of the page. Choose

the “Settings” option and select “Privacy”. In the section “Who can see my stuff?”, you can edit your desired settings.

You will now have four choices of how you want to protect your data. The first choice, “Public”, allows anyone to see all of your information. This is not advised. The second option, “Friends”, allows only the people that you have identified as your friends to Facebook. This is a slightly more secure option. The third option of “Only me” is designed to to make your posts completely private and only visible by you. The last option allows you to customize different areas of your profile so that different people can see different types of content. I only recommend this for advanced Facebook users. If you are going to use Facebook, select the “Friends” option. More importantly, make sure that the subjects listed on your friends list are people you really know and trust. Again I reiterate that if you put it on the internet, do not be surprised when it becomes public.

Many people have decided to completely delete their Facebook profile. They have discovered that this process is not as easy as it should be. Additionally, a Facebook account cannot be deleted right away. There is a “waiting period” of fourteen days. After the account is deleted, photos may remain on the Facebook servers for months or years. These photos are the legal property of Facebook. This may sound discouraging, but the sooner you begin deleting and stop adding additional information to Facebook, the better off you will be. If you are ready to pull the plug, the following are the proper steps.

- ✓ Log into your account and delete all of the content that you can. This includes all photos, messages, and interests. If you find something that cannot be deleted, replace the current data with bad information.

- ✓ Navigate to http://www.facebook.com/help/delete_account.

- ✓ Click on the “Delete My Account” button. This will technically deactivate your account in two weeks. If you log into your account any time within that period, your account could be reactivated.

- ✓ You will immediately receive an email from Facebook confirming the request.

- ✓ If you log into your Facebook account, you should receive a notification of a pending deletion. You can cancel or approve this request, but this step is not mandatory.

Facebook Likes Violate Privacy

I previously discussed methods of identifying a person's "Likes" on Facebook regardless of their decision to display them publicly in their profile. This was part of the pre-assessment conducted earlier. Other people can locate the items, businesses, pages and other "things" that you like on Facebook. I encourage people to refrain from clicking the like button anywhere. Consider the following scenarios.

- ✓ Courts have allowed the introduction of a person's interests from social networks as part of both criminal and civil cases. Imagine that you are the defendant in a civil dispute in reference to a traffic crash and your likes are "fast cars", "street racing", and "marijuana". None of this may have had any impact on the incident, but you will appear guiltier from the association.

- ✓ Attorneys have used a person's interests from online activity to create "jury appeal". Imagine that you are going through a bitter divorce proceeding and custody dispute. The opposing attorney presents the judge with your likes of a specific brand of beer, your favorite type of semi-automatic pistol, and your previous support of a politician that opposed the presiding judge's seat. While none of these interests are morally wrong, they definitely do not help your case.

- ✓ Many people jokingly like inappropriate topics on Facebook. I have seen police officers that "Like" prostitution pages, military members that associate with anti-military propaganda, and politicians that thought it was funny to click "Like" on pages associated with derogatory statements about mentally disabled individuals. The actions were done in jest, but the consequences of discovery are harmful.

- ✓ Finally, there is the consideration of first impressions. Before you meet for that first date, you are likely to conduct some online stalking research. What happens when the other person looks at your page? Will he or she know that you were not serious when you clicked “Like” for the Facebook fan page for the dentist that killed the protected lion in Zimbabwe?

Facebook Tagged Photos

If you possess a Facebook profile, anyone can post a photo of you to his or her own profile and “tag” you in the image. This will identify you in the photo by name and connect the viewer directly to your own Facebook page. Facebook gives you the ability to not only remove this tag, but you can also request removal of the entire photo. The following instructions will guide you through the process.

- ✓ Click on the down arrow in the far upper right of your profile while logged in to your Facebook account. Select “Activity Log”.

- ✓ Click “Photos” in the left column. Select the images that you would like to remove the tag from.

- ✓ Click “Report/Remove Tags” at the top of the page and select “Untag Photos” to confirm.

- ✓ If you would like the photo completely removed, choose the option “I want this photo removed from Facebook”. This will send a message to the user that posted the photo indicating your desire to remove the image. This is not mandatory to the user, but most people comply with this type of request.

Twitter (twitter.com)

Deleting your Twitter account is fairly straight forward. Go to your settings page. On the bottom of the account tab, there is a "Deactivate my account" link.

Click it, and confirm. Before you take the easy route, I encourage you to consider a few things.

If you have a Twitter profile with personal posts associated with it, there are dozens of websites that have collected all of your data and reproduced it. Deleting your account will not remove the posts that are replicated on third party websites. As an investigator, I am often presented a message on a suspect's account that says "Account deleted". This is usually due to the suspect learning that he or she is being investigated and the account is deleted out of panic. When I find this, I just go to a website such as Topsy (topsy.com) and pull up the user's posts. The next tactic will add an additional layer of privacy to hide your tweets.

Before deleting your account, remove every message that you have ever posted. Eventually, many of the third party websites that collect Twitter data will re-scan your profile and update the messages that are displayed on their site. Often, this will overwrite the information that is currently displayed with the current messages, which will be none. I prefer this over simply deleting the account. Also, when you delete your account, someone can open up a new account with your profile name after 30 days. With this method, you still have control of your account, there are no personal messages associated with it, and sites that collect your Twitter posts will collect your empty profile. Active Twitter users often have thousands of messages on their account. Removing each message individually can be very time consuming. Instead, consider an automatic message deletion option that will do the work for you.

Twit Wipe (twitwipe.com)

This service will remove all messages from your Twitter profile. In order to do this for you, the site will need your user name and password for your Twitter account. Before you provide this information, make sure that the password for your account is not associated with any other accounts. For example, if you use the same password for Twitter and your bank account, you do not want to provide anyone or any service that information. The chances of Twit Wipe disclosing this information are minimal, but do not take the chance. Change your password on Twitter to something unique. After you have a unique password for your account, navigate to twitwipe.com and log into your Twitter account. Confirm that you want the site to delete all of your messages and click the link

for “Start Wiping”. This can often take up to an hour. When the process is complete, and you have verified your messages are gone, change your password back to the original password of your choice on Twitter.

Google

I have a love/hate relationship with Google. I believe that it can be a great resource for anonymity when used appropriately and Google’s security is almost peerless. However, it can be very invasive when used with your real name and contact information. I will discuss the various ways to use Google products throughout this book. In this section, I will only discuss removal considerations.

The bad news is that Google stores absolutely everything. While there are scenarios that allow you to remove specific content from public view, the data continues to impact the overall disclosure of your account. The items that you post on Google products such as YouTube, Google+, and Google Photos will always have an association to your account. Consider the following test that I conducted.

I created a new Google account and obtained a new Gmail address. I then accessed this account from a new Android device and added five email addresses of people that I know to the contacts of the phone. I opened the Google Play store and immediately received information identifying the apps that these people use, their reviews of these apps, and the apps that they like. I expected this to happen as it is standard Google “sharing”. I immediately removed the contacts from my device, logged out of the Google account, rebooted the device, and logged back into this same account. While the contacts had been removed, Google remembered that I once knew these people and continued to allow me to see these types of data about them. Google never forgets.

Before proceeding, think about how this could impact you. It is likely that you have a Google account associated with your real name. It is also likely the primary account is connected to your phone if you use an Android device. With Android, you have probably downloaded numerous apps and possibly rated them or marked some as favorites. If this applies, anyone that has your email address in their contact list can see this information about you. Further, if a person has communicated with your email account in any way, the information described

here will populate their Google Play and Google+ profiles.

We must accept that Google knows the names, phone numbers, and email addresses of your friends and family through your Gmail account or Android phone. If you have emailed photos of yourself to any of these people, Google knows about that connection. If you have emailed inappropriate content, Google knows that too. Google knows what your interests and hobbies are, where you like to eat, and what movies you have seen lately. Google only cares about the ad revenue generated from this knowledge, but what happens if Google gets hacked? What if this information was leaked?

The more Google services you use, the more accurate and detailed this information becomes. I am concerned with what such a large amount of data represents. A rogue Google employee may use this data for nefarious purposes. Though their security is excellent, Google could be hacked. Worse, I have voluntarily and legally released this information to Google to use as they see fit by my acknowledgment of the Terms of Service. Further, Google would be obligated to release any collected content to any legal demand from any court. That is an unsettling and real possibility. Remember that anyone can be sued for practically any reason.

Therefore, I believe that any Google account that has been used in your real name, and connected to your real contacts, will always know and share more about you than you realize. I do not believe that you can sanitize these accounts to a state of anonymity. I can only recommend that you remove as much content as possible, and then consider alternative services. While I have used Gmail accounts associated with my real name in the past, I no longer use any Google services for personal communication. You should focus on content removal from non-email based services from Google.

YouTube: The only way to delete your YouTube account is to delete your Google+ profile. Before you take this action, you should delete your YouTube Channels. These contain the videos, comments, messages, playlists, and history within your YouTube account. The following steps will allow you to remove these containers.

- ✓ Sign into your Google account and navigate to

youtube.com/account_advanced.

- ✓ In the top right, click your account, then YouTube settings. Under the Account Settings, select Overview. Under each channel's name, select Advanced.

- ✓ At the bottom of each channel, select Delete channel and confirm.

This may take a few days to completely propagate. After you have confirmed that your channels have been removed, proceed to delete your entire Google+ account.

Google+: Google began integrating services into Google+ without user's consent. This has led to much confusion about how the social network should be used and has encouraged most users to seek alternatives. However, much of your personal details are likely present on some layer of this service. The directions below will completely close your Google+ profile.

- ✓ Navigate to google.com/account and select Data tools in the menu.

- ✓ Under the Account management section, click Delete Google+ profile.

Google Photos: The Google Photos app has been described as a way to upload and view all of your photos from any device. This obviously stores your content on the internet and is prone to leakage. Many people installed the app and decided it was not optimal for them. Unfortunately, simply installing the app allows Google to begin collecting your photos. Many people assume that deleting the app from your device will stop this behavior and remove your content. Upon deletion of the app, Google retains the photos that were synced. Further, it continues to collect your photos and add them to your profile unnoticed. The steps below will stop this behavior and remove your content from their servers. I can think of little else as private as your personal photos.

While these steps eliminate the photos from Google's live data set, it does not

remove them from the Google archive. Users can restore deleted photos within 60 days of removal. However, if you do not take any action to reverse these steps, the data should be unavailable after the 60-day period.

- ✓ From a computer, navigate to photos.google.com.
- ✓ At the top left corner of each photo, click the select icon. You can hold down the shift key to select an entire range.
- ✓ At the top right corner of the page, click the trash icon. This will move all selected photos to trash, which will completely disappear after 60 days.
- ✓ From your device, choose Google Settings and select Google Photo Backup. This location within your Settings menu will vary by the version of Android being used. It can often be found under Accounts. When located, toggle the switch to Off.

You should revisit your photos page a few days after you take these actions to ensure that new photos are not being shared. You may want to take a few test photos from your device and monitor closely.

Google Contacts: The contact information in your Google Contacts database is used by Google to associate you with the people you know. It is shared with every Google service and you cannot stop that. While Gmail is not a social network, it has several similarities. It is heavily integrated into Google's other services. I believe that you should think of the data in your contacts as a "Friends" list instead of an address book. Google uses this to disclose information about you to anyone that possesses your address in their list, similar to the earlier example.

This important data should always be exported before removal. You may regret simply deleting your contacts when needed later. I will export them in a way that they can be later imported into another provider. The following steps will create a backup of the content and then remove it from Google's databases. This should only be conducted when you are ready to leave Google as an email provider.

- ✓ Navigate to google.com/settings/takeout and click the Select none button.

- ✓ Enable the switch to the right of the Contacts option.

- ✓ Click Next at the bottom and follow the prompts.

This will create a small file in vCard format that will contain all of the data stored in your contacts. It can be used later to import this content into another email provider. You may want to take a moment and download all of the content from your Google account.

Google Now: This service is a voice activated personal assistant similar to Siri for the iPhone. Regardless of your opinion on the benefits of this technology, it should be noted that this data is visible to Google or anyone who has compromised your account through legal or illegal means. The following directions will identify the content being collected, remove undesired data, and disable future recording.

- ✓ Navigate to google.com/settings/accounthistory. Disable all options.

- ✓ When prompted, follow the prompts to delete the stored history of each service.

Google Account Removal

Some people simply want to delete their entire Google account. If you choose this option, I still recommend removing individual pieces of content using the previous methods. I do not believe that every reader should completely delete their Google accounts. Doing so will eliminate the ability to forward incoming email to a safer address. It may be sufficient to remove all content possible and forward all incoming email to a more secure alternative.

If you do not log directly into the account in any way, you prevent new data from being created from your usage. This is the route that I took. I had a Gmail

accounts associated with my real name and my previous phone. I eliminated all content throughout the Google architecture, forwarded my incoming messages to my new email provider, and never logged in again. Google collects minimal data from the incoming messages. These emails decrease weekly as people notice my new address from outgoing messages. However, some dedicated privacy enthusiasts may want to take it a step further.

If you no longer need the Gmail account associated with your Google profile, deleting the entire profile will eliminate all related data from Google's active environment. It may take a few weeks to purge out of all networks. In my experience, I was able to recover deleted data within 60 days of individual removal. However, I was unable to reactivate an entire deleted account. The following steps will eliminate all of your Google data associated with an individual account.

- ✓ Navigate to myaccount.google.com. In the Account preferences section, select Delete your account or services. Choose Delete Google Account and Data. Review the options and check both boxes at the bottom of the page. Choose Delete Account.

I should disclose one last time that this action is not reversible. Regardless of your certainty of these actions, I encourage you to download all of your Google content from their takeout website at google.com/settings/takeout. I can think of no logical reason to skip this phase of the process.

Instagram

Instagram makes account deletion easy. There is no need to remove individual posts or content. The following steps should permanently remove your entire profile from the internet.

- ✓ Navigate to Instagram.com/accounts/remove/request/permanent.

- ✓ Select any option from the dropdown menu explaining the reason for deletion and click "Permanently delete my account.

MySpace (myspace.com)

MySpace users are steadily leaving the service for more advanced networks such as Facebook and Twitter. These users leave behind an abundance of data that is being collected by dozens of data-mining companies. If you have ever created a MySpace page, you should consider completely deleting the profile to keep your photos, messages, and contacts from being passed around in public view. The official process is to log into your account, click on "Settings", and select "Delete Account". You can visit the MySpace privacy page at the following website.

https://myspace.com/pages/privacy

In my experience, this account removal process does not work. The request is ignored and nothing changes. However, I have found the following technique effective.

- ✓ Log into your MySpace profile and click the control panel and then "Profile". On this page, click on the "Basic" tab and change your year of birth to a year 12 years before today. This will make you appear to be 12 on your profile.

- ✓ The URL of the page that you are on will reveal your user number. It may look something like "http://www.myspace.com/4024450". Write down this number.

- ✓ Send an email to the law enforcement legal compliance division's account at compliance@support.myspace.com. Type "Underage User" in the subject line. Include a message similar to the following.

  > "My 12-year-old daughter has a MySpace profile stating she is 12. She is receiving unwanted contact from adults. Please remove this account immediately."

While this method is deceptive, it has worked. You are not breaking any laws by

using this technique on your own profile. MySpace will delete the profile immediately without question as a precaution.

LinkedIn (linkedin.com)

Many people have successfully used LinkedIn to gain employment and communicate with others in their industry. Most people that use this social network supply personal information to their LinkedIn profile including employment history, education, contact information, and various details that are often placed on a resume. I am most concerned with LinkedIn's terms of service that basically allow them to do anything they want with your content. Consider the following excerpt from their TOS as of December 2015 that outlines the permissions given to them.

"A worldwide, transferable and sub licensable right to use, copy, modify, distribute, publish, and process, information and content that you provide through our Services, without any further consent, notice and/or compensation to you or others."

If you are not comfortable with giving them practically unlimited rights to your entire profile, the following steps should remove your account from the internet. They will still likely posses your data provided up to this point, but it will eliminate any further leakage.

- ✓ Log into your account. Hover over the photo or photo placeholder of the account and select "Privacy & Settings". Click the "Account" link near the bottom of the page and navigate to "Helpful Links" and then "Close your account".

- ✓ Complete the Account Closure form and confirm the account that you want to terminate. LinkedIn will try to convince you to keep your account open a few times. When you successfully complete this process, you will be notified that an email will be sent confirming the deletion of your account. This may take up to a week.

Many people report that the account deletion confirmation never arrives. If this

happens to you, submit a help center request. Navigate to help.linkedin.com/app/ask. The website may automatically direct you to the help home page. If this occurs, you will notice access to the "Contact Us" link at the top of the page is blocked until you search for an answer. Simply search any term. Then after the results are displayed, you are allowed to click the link to "Contact Us". Complete this form with your information and an account deletion request. Be sure to include your profile number, which can be found in the address (URL) of your profile. In the address http://www.linkedin.com/profile/view?id=300972, the profile number is 300972.

Online Photos

A combination of cheap digital cameras and free online storage of photographs has created an enormous amount of personal information available to the public. Social networks and photo sharing websites encourage you to upload all of your photos and send the links to all of your friends and family. Many people have a false belief that only people that possess the direct links to the photos can see them. This is not true. Every one of these sites has a search function embedded into all of the pages that allows anyone to search for pages that may contain photos. The obvious risk here is that your personal photos will be seen by complete strangers. These strangers often include internet predators looking for images of children. The next concern is called the Exif data.

Exif Data

Every digital photograph captured with a digital camera possesses metadata known as Exif data. This is a layer of code that provides information about the photo and camera. All digital cameras write this data to each image, but the amount and type of data can vary. This data, which is embedded into each photo “behind the scenes”, is not visible within the captured image. You need an Exif reader, which can be found on websites and within applications. Keep in mind that some websites remove or “scrub” this data before being stored on their servers. Facebook, for example, removes the data while Twitter and Flickr often do not. If the image has been compressed to a smaller file size, this data is often lost. However, most photo sharing sites offer a full size view. The easiest way to see the information is through an online viewer.

Jeffrey's Exif Viewer (regex.info//exif.cgi)

I consider Jeffrey's Exif Viewer the online standard for displaying Exif data. The site will allow analysis of any image found online or stored on a drive connected to your computer. The home page, provides two search options. The first allows you to copy and paste an address of an image online for analysis. Clicking "browse" on the second option will open a file explorer window that will allow you to select a file on your computer for analysis. The file types supported are also identified on this page.

The first section of the results will usually provide the make and model of the camera used to capture the image. Many cameras will also identify the lens used, exposure settings, flash usage, date and time of capture and file size. This is a lot of data to share with the world.

Scrolling down the analysis page will then identify the serial number field. This is most common in newer SLR cameras and will not be present in less expensive cameras. This camera will identify the make, model, and serial number of the camera inside every photo that it captures.

ExifTool

I typically prefer local solutions over cloud-based solutions. ExifTool is a simple, lightweight tool that will quickly and easily display the Exif data contained on photographs. It runs in portable mode and does not require you to permanently install the application. To view Exif data for a photo simply open ExifTool and drag the photo onto the command line interface. A list of all available Exif data will be displayed. This tool can be used to see what metadata needs to be removed from the photo, and to verify that it has been removed before uploading. ExifTool is free and available by visiting owl.phy.queens.ca/~phil/exiftool/. A graphical user interface (GUI) that makes ExifTool easier to use, can be downloaded at http://u88.n24.queensu.ca/~bogdan/.

A serial number of a camera associated with an image can be valuable data. This can help someone associate photos that you "anonymously" posted to the

internet directly to you. For example, if I found a photo that you posted on your Twitter feed that you took with your camera, I may be able to identify the serial number of your camera. If I then find a photo that I suspect that you took but posted anonymously, I can see if the serial numbers match. I bring this up to explain the next threat.

Stolen Camera Finder (www.stolencamerafinder.co.uk)

This site was designed to help camera theft victims with locating their camera if it is being used by the thief online. For that use, you would find a photo taken with the stolen camera, and drop it into the site for analysis. This analysis identifies a serial number if possible. If one is located, the service then presents links to photo-sharing websites, such as Flickr, that contain photos with the same serial number. This can locate photos that you may not want to take credit for.

Camera Trace (cameratrace.com/trace)

An additional site that provides this service is called Camera Trace. Type in the serial number of a camera and the site will attempt to locate any online photographs taken with the camera. This service claims to have indexed all of Flickr, Twitter, Twitpic, Panoramio, and 500px.

GPS

Many new SLR cameras, and almost all cellular telephone cameras, now include GPS. If the GPS is on, and the user did not disable geo tagging of the photos in the camera settings, you will get location data within the Exif data of the photo. The data can display the analysis of an image taken with a camera with GPS. The data is similar to the previous analysis, but includes a new "Location" field. This field will translate the captured GPS coordinates from the photo and identify the location of the photo. Further down this results page, the site will display an image from Google Maps identifying the exact point of the GPS associated with the photo. All Android and iPhone devices have this capability.

Cropped Photos

Another piece of information that can be located from the Exif data is the presence of a thumbnail image within the photograph. Digital cameras generate a small version of the photo captured and store it within the Exif data. This icon size image adds very little size to the overall file. When a user crops the image, this original smaller version may or may not get overwritten. Programs such as Photoshop or Microsoft Photo Editor will overwrite the data and keep both images identical. Other programs, as well as some online cropping tools, do not overwrite this data. The result is the presence of the original and un-cropped image within the Exif data of the cropped photo. You can now see what the image looked like before it was cropped.

It is possible to delete or manipulate this Exif data. If you have a situation where it is necessary to upload photos to the internet, you may want to consider removing this metadata. This process is often referred to as "scrubbing" a photo. There are several ways to accomplish this.

If you have a computer that uses Microsoft Windows 7 as an operating system, you are ready to edit this data immediately. Locate an image on your hard drive and right-click the file name then select "Properties". This will present a new window with a tab titled "Details". Click on this tab and review the information. If the data attached to this image contains information that you do not want to share with the world, click on the link "Remove Properties and Personal Information". This will allow you the option to remove specific data from the image. I recommend selecting the "Select All" button to be sure that all of the Exif data is removed. If you are using a different operating system, there are several free applications that will remove this data.

Exif Remover (verexif.com/en/)

This website allows you to upload a digital image and either view or remove the metadata attached to it. Click on the "Browse" button, locate the photo you want to edit, and click "Remove Exif". You will be presented with a new download that will contain your image without the Exif data embedded.

Deleting Photo Sharing Accounts

Has this information motivated you to delete your photos uploaded to photo sharing networks? The following is a list of the most common services used in past years to upload and share photos. Many of these are no longer popular, but any content uploaded is still present today. If you do locate photos that need to be removed, you must log into the account that was used to upload them. If you did not create the account, you will need to contact the friend or family member that did.

You may find that your account settings on these photo sharing networks block your images from public view. I urge you to use caution with this restriction. In my experience, privacy settings only keep out the honest people. Hackers know how to bypass these and steal your content. Always assume that anything posted to the internet is public. Always choose strong privacy settings, but do not rely on them. Consider removing any undesired photos from the following accounts.

500px
Bayimg
Dayviews
DeviantArt
Flickr
Fotki
Fotolog
GifBoom
Imgur
Instagram
Ipernity
jAlbum
Lafango
Panoramio
Phanfare
Photobucket
Pinterest
Pixabay
Shutterfly
SmugMug
Snapfish
TinyPic
Vhoto

yfrog

What is so bad about online photos?

I place no photos on the internet. This is a very conscious decision based upon my view of privacy. I can think of many reasons why you might not want photos online, and the following may justify my harsh stance.

- ✓ Most private investigators will conduct a photo search before initiating any type of surveillance. If your adversary has hired a P.I. to tail you and document your activity, the absence of a public photo makes it a bit more difficult.

- ✓ Media outlets constantly scour the internet for embarrassing photos of subjects involved in the hot story of the day. I have seen journalists ignore respectful photos of someone in the news because of an unfortunate event and instead choose to show the most inappropriate option available.

- ✓ The photos available of you can be taken out of context. The image of you jokingly appearing unconscious at the bar years earlier may be used against you when you are seeking a position at a conservative company.

- ✓ Finally, you cannot take them back. We must assume that anything posted to the internet stays there forever in some form. Decisions today to post images online cannot be reversed later when desired. Proactive policies on removing current photos, and eliminating future images, might benefit you drastically some day.

Google Maps (maps.google.com)

Unless you live in a very rural area or at the end of a mile-long private drive, a street view of your house is probably on the internet. Google has been taking 360 degree photos from every street in the country for years. People can then use the Google Maps website to see images of a residence or business. This often identifies personal and work vehicles, physical security vulnerabilities, and occasionally family members standing in the yard. Many people assume that there is nothing that can be done about this. Removing these images is quite easy.

- ✓ Navigate to the Google Maps website and type in your home address. There will be a red marker on the map hovering over your house. Click on this marker and look at the options in the popup menu. If there is a street view of your house, this option will appear in this window. Click on the Street View link to open a new view which can be moved and zoomed with the mouse.

- ✓ On this new view, manipulate the image so that you can see your house on the screen. On the lower left portion of the image, there is a link titled “Report a problem”. Click on this link and view the resulting page.

- ✓ The first section of this page asks “Why are you reporting this street view?”. Select “Privacy Concerns”, and then “My House”, and then “I have found a picture of my house and would like it blurred”. In the next section, enter your privacy concern which can be “I have found a picture of my house and would like it blurred”. Enter your anonymous email address and make sure that the red box on the image below is surrounding your house. Complete the word verification and click “Submit”.

I have heard about success stories and failures. Some people have reported that they added one of the following lines in the description window to obtain immediate removal.

- ✓ “Photo identifies a building used for home-schooling students”. I like this one. Most likely, you have taught a child something in your home at some point. Technically, you were home-schooling.

- ✓ “Photo identifies physical security vulnerabilities of the building”. This one is a great catch-all as well. Every building has a physical vulnerability such as a door lock, windows, or attic vent. Your home should qualify for this.

- ✓ “Photo identifies home of a police officer targeted by violent criminals”. For the law enforcement community, this seems to get their attention. It should be obvious whether this applies to you or not.

Blogs

A personal blog is a website where a user can publish personal content. These are often compared to a diary kept in public view. They are popular with teens and young adults. Often, the site will include text, photos, and videos. The text is usually personal and occasionally discloses information that is later regretted. The most common free blog services are provided by Tumblr, Blogger.com, WordPress.com, and Blog.com. The method of deleting a blog is different on each service and is outlined below.

Tumblr

This Yahoo owned service is now the most popular blogging website. Millions of users upload billions of posts for the world to see. Some of this is innocent, some intrusive, some illegal, but all removable. The following steps will permanently remove your account.

- ✓ Log into Tumblr at tumblr.com and visit your settings page from the left corner.

- ✓ Scroll to the bottom and choose Delete account

Blogger (blogger.com)

Blogger, owned by Google, does not give you the option to delete your blog after

it has been published. There are no options in your account settings that allow you to close your account. Instead, you must take a manual approach.

- ✓ Log into your Blogger profile. This will be the same credentials used to log into your other Google accounts, and you should be automatically logged in if you are already signed in to any Google service. You should be directed to your Blogger Overview page. If not, click on “My Blogs”. Click on “Posts” on the menu on the left of the page. This will present every post published on the blog. Select each box next to each post and then click the trash can icon in the upper middle.

- ✓ Edit your profile to remove any personal information stored there. For required fields, you can enter false information. To access this content, click on your user name in the upper right corner of any blog page. This will present a menu with an option of “Account Settings”. Click this and remove or edit personal data.

- ✓ Change your user name on Blogger to something not related to you. I recommend random characters. This will prevent any association to you.

WordPress (wordpress.com)

Similar to Blogger, WordPress will not let you delete your account. They will allow you to delete any individual blogs though.

- ✓ Log into your WordPress profile page and click on the “My Blog” tab. This will provide a list of all blogs that exist in the account. Click on the “Dashboard” link under each blog.

- ✓ Highlight the “Tools” option on the left menu. This will present a link titled “Delete Site”. The next page will ask for a reason for this action. Choose the last option of “Permanently delete the blog name and all content”. Check the box to confirm this action and click the button to execute the removal.

- ✓ Check your email account that was used to originally create the blog. You will receive a verification email that will include a link to confirm the removal. Repeat this process for any other blogs in the account.

Blog (blog.com)

Until recently, the only option for removing a personal blog on this site was to submit a help ticket and request removal from customer service. You can now complete this on your own account.

- ✓ Sign in to your account on blog.com. On your dashboard, click "Settings" and then "Delete Blog". This will present a large button titled "Delete My Site Permanently". You will receive an email at the address that you used when creating your account. Click on the verification link in this email to confirm the deletion.

Social Network Search Sites

Now that you have removed all of your social network presence, you may think that you are ready to move on to another topic. Unfortunately, there is more to discuss. While your personal information is no longer visible on the social networks where it was posted, it has been collected and archived by other companies. These social network aggregators maintain their own copy of the public data that was visible on your profiles from Facebook, MySpace, Twitter, and others. The methods described in the next chapter will remove the data collected about you.

Everything Else

There are hundreds of social networking websites. They each have their own method for proper account deletion and few of them make these instructions easy to find. Two online services are available to help you discover the preferred way to delete a specific account. Account Killer (accountkiller.com) and Delete Your Account (deleteyouraccount.com) both offer detailed instruction on deleting hundreds of different accounts. Check these sites, enter the name of the

website from which you want your data removed, and follow the instructions. If you have a rare site that is not mentioned here, conduct a search on a couple of search engines and you are likely to find everything you need.

Many of you will find that you have never opened a social network account, yet there are many personal details out there about your family. This is often posted by parents, siblings, and children. You will not be able to take direct action against an online profile that you do not have access to. If you want the data removed, you will need to approach the friend or family member that posted the content.

The box on the following page was designed to assist with the identification and removal of sensitive content from within social networks. Knowing the date searched and whether you found a result or not might be useful later when revisiting the content. Placing a check mark next to each result can indicate that the data was later removed. While not complete, it provides the most common networks where you may have an undesired presence.

Date:	Result:	Network:	Address:
Social Networks			
_____	_____	Facebook	facebook.com
_____	_____	Facebook Photos	facebook.com
_____	_____	Facebook Comments	facebook.com
_____	_____	Twitter	twitter.com
_____	_____	Instagram	instagram.com
_____	_____	LinkedIn	linkedin.com
_____	_____	MySpace	myspace.com
_____	_____	Google+	plus.google.com
_____	_____	Tumblr	tumblr.com
_____	_____	YouTube	youtube.com
_____	_____	Reddit	reddit.com
_____	_____	Vimeo	vimeo.com
_____	_____	Pinterest	pinterest.com
_____	_____	Foursquare	foursquare.com
Blogs			
_____	_____	LiveJournal	livejournal.com
_____	_____	Blogger	blogger.com
_____	_____	Blog	blog.com
_____	_____	Wordpress	wordpress.com
_____	_____	Disqus	disqus.com
_____	_____	ISSUU	issuu.com
Photos			
_____	_____	PhotoBucket	photobucket.com
_____	_____	Flickr	flickr.com
_____	_____	Fotki	fotki.com
_____	_____	SmugMug	smugmug.com
_____	_____	ShutterFly	shutterfly.com
_____	_____	Panoramio	panoramio.com

Chapter Ten

Web Publishing

You may expect this chapter to simply advise against any type of publishing of online content. This is not the case. I possess multiple websites, own several domains, publish to blogs, and have a minimal online presence. I respect the requirement for activity on the internet in order to maintain a business or generate income. Some may use the internet as a tool to complement their professional life. This may apply to attorneys, aspiring politicians, software developers, or physicians.

While not appropriate for everyone, running a web based business actually has some great privacy advantages over traditional employment. The biggest benefit is the lack of a requirement for you to expose your personal details to an employer. Most companies will demand government identification, a verified home address, your SSN and DOB, as well as a complete history of your previous employment. While this step alone might seem invasive, the potential attacks after that company is breached could be devastating. I am forced again to reference the OPM breach. If you create your own online business as a source of primary or secondary income, you control the data that is made public. I hope that you will consider the option of working for yourself. This chapter will provide insight to the ways your data is leaked through online publishing.

This chapter is not only for those desiring self employment. It is likely that you have a legitimate purpose for publishing some type of content to the internet. Whether it is your own website hosted on a domain that you own or a blog hosted on a third party service, you should be very cautious of the registration process. Many people realize that their details are publicly viewable after the damage is irreversible. This mostly applies to domain registration which is where I will begin.

Domain Registration

Delivering online content through your own website hosted through your own domain can be very satisfying. It also gives you compete control of your website, the data collected, and the data shared. I host all of my content. This gives me the option of offering very transparent privacy policies that assure my visitors that I am not tracking them or collecting their information. The first step of hosting your own website is to register the desired domain name. The process for this will vary based on the service that you use to register the domain. I will only focus on the privacy aspects of registration.

Every registered domain is required by The Internet Corporation for Assigned Names and Numbers (ICANN) to include the following information for the primary registrant and technical, administrative, and billing contacts if not the same as the registrant.

Full Name
Full Address
Telephone Number
Email Address

Many readers will assume that one could simply provide false information and move on to the next step. Unfortunately, it is not that easy. The email address that you provide must be valid and retrievable by you. The remaining information will likely never be verified. However, if a complaint is received about your registration by ICANN, they will require you to verify the supplied information or update to valid details. While this is rare, I do not suggest blatantly lying about your information.

Every domain registration service will allow you to change your registration information at any time. However, this does not protect previously supplied details. An example of this can be seen on the website whoisology.com. This website extracts domain registration data and stores the historical changes. The domain name inteltechniques.com is currently registered to a PO Box in Washington, D.C. However, it was previously registered to a physical address in Alton, IL. While the record was updated, there is nothing that can be done about the previous entry. It is publicly visible forever. I have had many clients contact

me to inquire of the process of removing this data. The unfortunate answer is that this cannot be undone. Therefore, it is vital to register the domain properly the first time.

If the website content is publicly attached to your real name, I see no issue with registering the domain in your name. The address should never be your home or workplace. It should never be anywhere that you could be located routinely. PO Boxes are allowed here, but I suggest caution there as well. I do not recommend using the primary PO Box that you use for bills and personal correspondence. You are likely to begin receiving unwanted advertisements. While not a privacy issue, it can be annoying. My bigger concern is directed toward the routine collection of mail at this address. If you visit your PO Box daily or weekly, it would not be difficult to be located during this process. This may not be important to most, but it is to those that desire ultimate privacy. Personally, I do not want to provide a private investigator, process server, or stalker all of the information needed to find me through public domain registration data. I also do not recommend using the address of your employer. You have other options.

The first is a secondary PO Box. I have one. They are only used for situations where I never expect to receive any mail, but might be required to verify ownership. I never physically check them. They are in rural towns and cost about $50 per year.

The next option is to pay for private registration. This allows your company that you registered the domain through to act as the contact. They are the public face and will forward any inquiries directly to you via email. My concern here is two-fold. You are required to share your true contact information with the domain registrar. What if they get hacked? Second, these services are facing scrutiny from ICANN and there is a solid possibility that these masking services will be banned in the near future. It would not surprise me if they are forced to share historic contact details. I do not recommend this route.

A final solution is to simply use someone else’s address as the contact. I do not recommend picking a random stranger out of a phone book. Instead, consider the address of the provider of your domain. If you registered for a website domain through GoDaddy, use their address. I believe that you have that option as their customer. If ICANN tries to reach the owner of your domain by contacting

GoDaddy, you can be reached via email. However, using the same address as provided on the godaddy.com domain registration, 14455 N Hayden Rd Suite 219, Scottsdale, AZ, is not wise. It may raise a red flag. A quick search on the internet reveals that GoDaddy's Global Technology Center is located at 2150 E Warner Rd, Tempe, AZ. A GoDaddy customer may choose to use that. I believe that you meet the requirements of the registration by providing your real name, GoDaddy's address, a forwarding email address (33 Mail), and a VOIP number.

Search Engine Control

When discussing the topic of search engines indexing your website, most people will do anything they can to convince Google, Bing, and others to collect as much information as possible. They hope to have a high ranking and for their website to appear first in a search result. The strategies for this Search Engine Optimization (SEO) are beyond the scope of this book. Instead, I will discuss the opposite. I want to make my website as private as possible while maintaining a healthy presence within search engine results.

Websites possess special instructions to search engines in the form of a small file stored at the root of the website called robots.txt. This text file contains specifically formatted written instructions to the search engines that crawl your website. It will allow you to block specific content from being reported, restrict archiving permissions, and other desired requests. The following will explain the options, and I will display an ideal robots.txt file.

First, you must store the file at the proper location. It should be at the base of the domain, formally known as the root folder. As an example, you can view the robots.txt file by adding a slash and the file name after any domain. Below are a few examples, one more interesting than others.

inteltechniques.com/robots.txt
google.com/robots.txt
tripadvisor.com/robots.txt

I will create a new file in any text editor and save it as robots.txt. The first decision to make is the extent that you want search engines to look through your

website. If it is all public, you may include the following line.

```
User-agent: *
Disallow:
```

The first line uses an asterisk (*) to indicate that this rule applies to any and all search engines. The second line is empty after Disallow indicating that it does not request to block anything. Everything is allowed. If you do not want the search engine to look at your website or include any links to it, you would include the following line of text.

```
User-agent: *
Disallow: /
```

The option of a forward slash (/) indicates that you want to disallow everything on the site. If you wanted to only block a folder titled “Private” on your domain, the text would be the following.

```
User-agent: *
Disallow: /Private/
```

If you had a single file on the root of your website, such as private.html, that you did not want any website to index or include in search engine results, you would include the following.

```
User-agent: *
Disallow: /private.html
```

I never recommend this specific strategy. While search engines will not display a link to that page, anyone could view your robots.txt file and navigate straight to the desired content. You may have specific types of files to protect, such as those ending in .aspx. You could add the following to protect that content.

```
User-agent: *
Disallow: /*.aspx$
```

The asterisk (*) and the dollar sign ($) indicate that all files with that extension should be avoided. If you wanted to only prevent Google from indexing your content, but wanted any other search engine to proceed, you could include the following.

```
User-agent: Googlebot
Disallow: /
```

I do not recommend citing any specific search engines. I believe that it is all or nothing. Either you block all engines or you block none. This prevents the creation of a robots.txt file that contains errors or contradictions.

While these techniques are important for control of your website data that is present on search engines, I have a much more vital consideration. When your website is indexed, it is also collected and archived. Google, Bing, the Wayback Machine, and others capture a snapshot of your page and offer it as a cached file. As an example, consider the website fbi.gov. You have several options for viewing this content. Typing fbi.gov into a web browser will present the live site as it appears today. Searching Google for fbi, clicking the downward facing green arrow next to the first result, and clicking “Cached” will present a copy of fbi.gov that was recently captured by Google. Repeating this process on Bing will produce the same results. If fbi.gov were to shut down today, you could still acquire the copies collected by Google and Bing.

The Wayback Machine goes a step further. It not only collects website data similar to Google and Bing, it allows users to see all of the content collected. Searching fbi.gov on archive.org/web discloses that the Wayback Machine has collected the contents of the fbi.gov website over 6,000 times since 1996. Clicking any result allows you to view the website as it appeared on any given date. In contrast, repeat the previously mention steps on the domain inteltechniques.com. You will notice that Google, Bing, nor the Wayback Machine possess any cached copies of this website. This is due to a single entry of text with the robots.txt file of that website. The following prevents websites from collecting, or caching, the content.

```
User-agent: ia_archiver
Disallow: /
```

As a final example, assume that you have a website that you want to be indexed by all search engines. You want people to be able to search for you and your content. However, you have a folder titled “Hidden” that you do not want crawled. Finally, you do not want search engines to store copies of your data and make them publicly viewable forever. The following would be your robots.txt file.

```
User-agent: ia_archiver
Disallow: /

User-agent: *
Disallow: /Hidden/
```

I believe that you should consider this proactive approach rather than a reactive approach. As you can see, the internet never forgets. If you find yourself in the spotlight due to an unfortunate event, your entire web presence will be scrutinized. While you can take down your website, you cannot immediately remove the data collected during search engine indexing. If you forbid engines from caching your data in the beginning, you have much more control of the available views at all times.

If a search engine has already collected and exposed undesired content from your website, you do have options for removal. There are two basic strategies, and I will explain both for Google and Bing. The first idea is to delete the content and ask the search engines to re-scan your site. When they do, and see that the data is no longer present, they will eventually remove the dead link and the attached cached file. This is the easiest approach and does not require an account. The following will explain the steps for Google and Bing.

Google: Navigate to www.google.com/webmasters/tools/submit-url and enter your domain. They should re-index within two days.

Bing: Navigate to www.bing.com/toolbox/submit-site-url and enter your domain. They should re-index within one day.

With this method, you are at the mercy of Google and Bing’s response. This is

not immediate, and they may not respond to your request. The next options require more work and setup, but also receives a better response.

Google: Navigate to www.google.com/webmasters/tools/home and create an account. You will need to add a verification file to your website host which can be removed when complete. This site can instruct you on this procedure. Navigate to www.google.com/webmasters/tools/url-removal and select the search results from your website that you want to remove.

Bing: Navigate to www.bing.com/toolbox/webmaster and create an account. You will need to compete the verification process to prove that you own the domain. Choose “Block URLS” within the “Configure My Site” section and enter the pages that you want immediately removed.

After you have achieved the desired results, I recommend that you remove any files that Google or Bing had you place on your website. While this does not give these services direct access to hidden data, it does allow more in-depth tracking of visits and content.

If your website has been on the internet for a while, and the Wayback machine possesses several copies in its collection, you can remove them all. Simply add the “User-agent: ia_archiver” line mentioned previously to your robots.txt file. When the Wayback machine crawls your site, it will see this command and complete two actions. It will identify your site in its database of domains to exclude from search and will remove all stored entries from its archive. Depending on the overall popularity of your site, this should happen within a week.

Chapter Eleven

Government Records

Government records contain some of the most sensitive pieces of information about you. Information about your finances are contained in your tax records. Data about your date and place of birth and parents is contained in your birth certificate. Your place of residence is purposefully recorded by the city, county, and state you will live in. The politicians you support financially and vote for are present in these records. If you have a permit to carry a concealed handgun, this information is recorded. In some states, it is considered a matter of public record along with your home address.

Opting out of most of these records is not possible. The government will not allow you to simply remove the record of the purchase of your house. Though this would certainly enhance your privacy, it would make it much more difficult for your city, county, and state to collect taxes on you. The strategies for dealing with these types of records may vary from state to state, and from town to town within a given state. There is no single check listed approach that I can offer that will work in every jurisdiction in the United States. Consider this chapter as a set of guiding principles rather than a collection of guaranteed techniques.

Public Records

While reading this book, you have probably found your home address, telephone number, and family member’s names on the internet. Most likely, this data was collected at some point from public information. From there, it has spread to dozens of websites and marketing lists. In order to prevent your information from re-appearing on these websites, you must make some changes to your public profile.

Some of the most vital information that you should protect from public view is data that everyone has legal access to. If you think that your date of birth, divorce records, voter records, traffic offenses, and civil litigation are protected, you are wrong. This is all public data and there is nothing stopping individuals and private companies from collecting your information and selling it to anyone that wants it. This is not the end of the chapter though. Just because something is a part of the public record, it does not mean that you cannot make it difficult to find. This chapter will help you reverse some of the damage that is already out there, but your future actions are more important.

Property Tax Records

I believe that the most important data to consider in reference to privacy is your property taxes. Most likely, you own a home and you pay yearly property taxes. These may be incorporated into your house payment. Your property taxes will likely be in your or your spouse's name, or maybe both. This single record will announce your home address to the world. The numerous people search sites that were discussed in Chapter Eight rely on these records to locate people and charge a fee to disclose your location. Having an unlisted telephone number does not hide this data. There are two approaches to fixing this problem, and I recommend applying both.

Data removal

Because the tax records are public, you cannot request the information be removed from public view. However, you can request that the information is removed from the online database. Each county has a database that stores the property tax records. Most of them make this data available online through the county website. The companies that have been discussed here know how to collect all of that data and add it to their own data set. This data is more reliable in locating people than telephone directories or social networks. You cannot remove the records yourself. You will need to contact the county in a very specific way.

- ✓ Conduct a search on the internet for your county's property tax database. If you live in Cook County, Illinois, your search may look something like "Cook County IL property tax search". For most

counties, this will display some type of database that can be searched by name, address, or parcel number. Search your own information and make note of the parcel number and a telephone number for the Clerk's office.

- ✓ Telephone your County Clerk's office and politely make the following request:

  "I have noticed that my personal information and address are visible on your property tax website. I realize my property tax records are public records and must be made available to anyone that wants to personally view them, but I would like to have the online records removed. I have recently discovered several websites that have extracted the information from your database and made it available for the purpose of locating people."

- ✓ Continue the conversation and include any other reason to enforce the removal request. This can be any of the reasons identified in Chapter Eight that may make you more vulnerable to danger. Below are four examples.

  "I am a (choose one) police officer / public official / community leader and possess a higher risk of danger from the community."

  "I have been the victim of identity theft and I am removing my personal information from data mining companies in order to prevent further criminal activity"

  "I have been a victim of a violent crime and fear for my safety. The ability to locate me based on your online records has increased the danger of bodily harm"

  "I have been the victim of threats and harassment. The ability to locate me by searching your online database places me in immediate danger of bodily harm."

Choose your response wisely. You may be asked to provide proof of your claim. Subjects that attend my training sessions have notified me that proof of their statements were never requested. Some attendees have stated that they received great resistance in these telephone calls and were occasionally told that the request was impossible. If this happens, call again and request the Information Technology (IT) division. Repeat the above process to them. Most likely, a computer professional will be the person that will ultimately be responsible for removing the information. Attendees have confirmed that this second call was successful.

Removing your information from this online database is a huge victory. However, this does not hide your address from the public completely. It also does not remove your information from companies that have already obtained the data. The previous chapters should help with that. It will prevent data mining companies from getting easy access to it, but someone can still find you with a personal visit to the County Clerk's office. Most likely, a helpful employee would even conduct the search for them and offer to write down or copy the information. My recommendation is to never have your property taxes in your name.

Ownership Change

If you plan on living in your current home for the next several years, you may want to consider legally changing the owner of your residence to a living trust. This will also change your property taxes to the name of the trust. Before you do this, you must establish a living trust for yourself and your spouse. The full details of establishing a living trust are far beyond the scope of this book. There are many great books that will help you accomplish this, and many people complete the process without the guidance of an attorney. Here are a few of the benefits.

- ✓ You can place any assets in a living trust including real estate, investment accounts, and personal property in your home.

- ✓ Having all of your assets in a living trust can keep your assets out of probate, which provides a great layer of privacy.

- ✓ It will give you complete control of what happens to your assets when you die without making the details public.

- ✓ The trust can be amended at any time or completely revoked.

- ✓ You can name your trust anything you want. It does not need to include your name, and I do not recommend identifying yourself or your family in the name of the trust. It could even be “Hiding from the Internet Living Trust”.

After you establish a living trust, you can contact the County Recorder in your county to change the ownership of your property. In my county, the fee was $41.

New Ownership

If you are planning on purchasing a new home or making any permanent move, this is a huge opportunity to make it practically impossible to be located. This method is only for those of you that are truly committed to being invisible from the public. The general idea of this process is credited to J.J. Luna, the author of the book ***How to be Invisible***. This book is considered by many to be the definitive guide to removing yourself from public view. A new edition was released in 2012. The basic premise of this specific method is the following:

- ✓ Purchase an official LLC from a registered agent in New Mexico. These are never publicly associated with your real name, but you own the business.

- ✓ Purchase your new home using the LLC as the owner. The LLC can also purchase vehicles and other property.

- ✓ Never associate your name with the house you live in. Personal mail should be delivered to a PO Box. Utilities should be in the name of the LLC.

If you are at all intrigued by these possibilities, purchase Luna’s book

immediately. The methods are completely legal. If you are in any way targeted by the public, such as police officers or victims of harassment, this will guarantee that you will have a safe home.

Internal Revenue Service

You have likely heard about criminals filing false tax returns and claiming unauthorized refunds from identity theft victims' filings. This has become a multi billion-dollar problem for the IRS. It is obvious that your tax records are not completely protected, and you have no choice but to allow storage of your details such as SSN, DOB, address, and income. However, you can control some data provided. You can also eliminate unauthorized filings. I recommend that everyone consider the following as mandatory practice.

- ✓ File before the fraudsters do it for you. Your primary defense against becoming the next IRS scam victim is to file your taxes at the state and federal level as quickly as possible. This is usually the second or third week in January. It does not matter whether or not the IRS owes you money. Thieves can still try to impersonate you and claim a refund.

- ✓ File IRS form 14039 and request an Identity Protection (IP) PIN from the government. This form requires you to state you believe you are likely to be a victim of identity fraud. I believe that all Americans have been impacted by incidents that could lead to ID theft. This form can be found on the IRS website.

Voter Registration Records

If you are a registered voter, your home address is visible to the public. Most likely, there is a database on your county's website that will list every registered voter's home details for the entire county. It identifies a person's full name, home address, dates voted, and political affiliation. Data mining companies know about these and use them to collect information about you. Removing this information is vital to protecting your privacy.

- ✓ Navigate to blackbookonline.info/USA-Voter-Records.aspx and select your state. On the next page, select your county. This will forward you to the online voter database for the county you live in. Some counties do not have online access yet.

- ✓ Search for your name in the database. If you locate your records, it will probably identify both your residence address and a unique number associated with your voter record. Make note of this number. It will also likely display each date that you have voted in either local or national elections.

- ✓ Contact your County Clerk's office and request to add your voter registrations information to the "Address Confidentiality Option". This can be done at the same time you request the removal of your property tax information from the online database. This option was originally designed to help participants keep their home address secret. Most people that take advantage of this program are victims of violent crime, harassment, or identity theft. If this request is denied, request an address change and provide your PO Box information.

Military Recruiting Databases

Section 9528 of the No Child Left Behind Act of 2001 requires all school districts to release student names, addresses, and telephone numbers to all military recruiters. If you do not want military recruiters to add your child to their recruiting database, you can demand that the school not release the information. This removal option is a part of the Family Educational Rights and Privacy Act (FERPA), but is rarely offered.

- ✓ Navigate to leadps.org/images/content/479/Military_OPT-Out.pdf and print the form. This form only requires the school name, student name, student signature, and parent signature. Figure 11.01 displays a portion of this form.

- ✓ Deliver this form to any schools that your child attends.

I, _____, hereby exercise my federal right, granted to me by the Congress of the United States under Section 9528 of the *Elementary and Secondary Education Act of 1965*, as amended by the *No Child Left Behind Act of 2001*, (and any other applicable state, federal or local law or any school policy), and hereby request that the name, address, and telephone listing of _____, a current student at _____ High School, not be released to military recruiters without prior written parental consent. I do, however, consent to the disclosure of such information to institutions of higher education other than military schools.

Figure 11.01: The removal options of a FERPA form.

Aristotle (Aristotle.com)

This website relies on public records to assist in political campaigns. This includes voter records and county data. If you located your personal information on any county website, Aristotle has your data for sale. A removal request is accomplished through email.

- ✓ Create a message to remove@aristotle.com. In the body of the email, state that you request "Any and all information associated with the following person removed from all online and offline databases maintained by Aristotle". Include your full name and home address.

Court Records

Civil and criminal court records are public information. Anyone can visit their county court and search local court cases on county owned computers. Most courts have uploaded this live database to the internet. A quick search on my county's court database identified profiles by subject name which included civil cases, traffic offenses, misdemeanors, and felonies. There is very little that you can do about information in your profile. You should visit the following website and select your state of residence.

blackbookonline.info/USA-County-Court-Records.aspx

Select your county and visit the county's online court database. Search your

name and verify any cases that you are involved in. If you have only one offense, you can contact the state's attorney's office for your county and request an expungement form. If the expungement is approved, the details of the event will be removed from all court databases. This will not remove the data from any private websites that possess a copy of the archive. Below is a list of websites that provide court records for a small fee. If you want to be sure that your expunged case is removed from these websites, visit the link for contact information.

usabackground.com
completebackgroundchecks360.com
www.courtrecords.org
courtregistry.org/index.php
courtclick.com/terms.php
criminalpages.com/optout
criminal-records.org/privacy.php
datadetective.com/privacy.php
detectiveunlimited.com
publicbackgroundchecks.com

Privacy Act Requests

The Privacy Act of 1974 establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies. You have the right to request your own record. If your files contain anything classified or deemed inappropriate for release, they will be redacted. I have found the following letter helpful for a successful response containing your personal files, followed by three agencies that you may want to contact. This can also be sent to the FOIA division of any federal agency.

This is a request for records under the provisions of the Freedom of Information Act and the Privacy Act. Please process this request under both statutes to release the maximum number of records. I request copies of all personal files, correspondence, or other records.

My full name:

My date of birth:
My place of birth:
My Social Security number:

Under penalty of perjury, I hereby declare that I am the person named above and I understand that any falsification of this statement is punishable under the provisions of Title 18, United States Code (U.S.C.), Section 1001 by a fine of not more than $10,000 or by imprisonment of not more than five years, or both; and that requesting or obtaining any record(s) under false pretenses is punishable under the provisions of Title 5, U.S.C., Section 552a(i)(3) as a misdemeanor and by a fine of not more than $5,000.

Information Coordinator
Central Intelligence Agency
Washington, DC 20505

Federal Bureau of Investigation
Records Dissemination Section
170 Marcel Drive
Winchester, VA 22602-4843

United States Secret Service
FOIA / PA
245 Murray Drive, Building 410
Washington, DC 20223

Concealed Carry Permits

Most states in the US allow the issuance of concealed carry handgun permits to qualified citizens. The laws in each state vary and it is up to you to know your own state's regulations regarding legal concealed carry. Each state also varies in how it handles the information of concealed carry permit holders. In some states, this information is considered a matter of public record and may be requested by the media or by individual citizens through a Freedom of Information Act request. The accompanying chart shows each state's stance on protecting the privacy of concealed carry permit holders. The extent of the information to which these states will give out, and to whom they will give them varies state-to-state. If you have questions about your own state's laws regarding your privacy as a concealed carry holder, consult the applicable law listed in the chart.

State	Public/Private	Applicable Law
Alabama	**PUBLIC**	Alabama Public Records Law
Alaska	PRIVATE	Alaska Public Records Act
Arizona	PRIVATE	Arizona Public Records Law
Arkansas	**PUBLIC**	Arkansas Freedom of Information Act
California	**PUBLIC**	California Public Records Act
Colorado	**PUBLIC**	Colorado Open Records Act
Connecticut	PRIVATE	Connecticut Freedom of Information Act
Delaware	PRIVATE	Delaware Freedom of Information Act
Florida	PRIVATE	Florida Sunshine Law
Georgia	PRIVATE	Georgia Open Records Law
Hawaii	PRIVATE	Hawaii Uniform Information Practices Act
Idaho	**PUBLIC**	Idaho Public Records Act
Illinois	PRIVATE	Illinois Freedom of Information Act
Indiana	**PUBLIC**	Indiana Access to Public Records Law
Iowa	**PUBLIC**	Iowa Public Records Act
Kansas	**PUBLIC**	Kansas Open Records Act
Kentucky	**PUBLIC**	Kentucky Open Records Act
Louisiana	PRIVATE	Louisiana Sunshine Law
Maine	**PUBLIC**	Maine Freedom of Access Act
Maryland	**PUBLIC**	Maryland Public Information Act
Massachusetts	PRIVATE	Massachusetts Public Records Act
Michigan	PRIVATE	Michigan Freedom of Information Act
Minnesota	PRIVATE	Minnesota Data Practices Act
Mississippi	**PUBLIC**	Mississippi Public Records Act
Missouri	PRIVATE	Missouri Sunshine Law
Montana	**PUBLIC**	Montana Public Records Act
Nebraska	PRIVATE	Nebraska Public Records Law
Nevada	**PUBLIC**	Nevada Open Records Act
New Hampshire	**PUBLIC**	New Hampshire Right to Know Law
New Jersey	PRIVATE	New Jersey Open Public Records Act
New Mexico	PRIVATE	New Mexico Inspection of Public Records Act
New York	**PUBLIC**	New York Freedom of Information Law
North Carolina	**PUBLIC**	North Carolina Public Records Law
North Dakota	**PUBLIC**	North Dakota Open Records Statute
Ohio	**PUBLIC**	Ohio Open Records Law
Oklahoma	PRIVATE	Oklahoma Open Records Act
Oregon	PRIVATE	Oregon Public Records Law
Pennsylvania	**PUBLIC**	Pennsylvania Right to Know Act
Rhode Island	**PUBLIC**	Rhode Island Access to Public Records Act
South Carolina	**PUBLIC**	South Carolina Freedom of Information Act
South Dakota	PRIVATE	South Dakota Sunshine Law
Tennessee	**PUBLIC**	Tennessee Open Records Act
Texas	**PUBLIC**	Texas Public Information Act
Utah	PRIVATE	Utah Government Records Access and Mgmt Act
Virginia	**PUBLIC**	Virginia Freedom of Information Act
Washington	PRIVATE	Washington Public Records Act
West Virginia	**PUBLIC**	West Virginia Freedom of Information Act
Wisconsin	PRIVATE	Wisconsin Open Records Law
Wyoming	PRIVATE	Wyoming Sunshine Law

Chapter Twelve

Disinformation

The first edition of this book made a brief mention of what many people refer to as misinformation. Technically, misinformation is when a person unintentionally provides inaccurate information which causes inappropriate content to be released or replicated. Most people are really talking about disinformation. This is when a person intentionally provides false or misleading information with an attempt to create inaccurate data. Disinformation is exactly what we want to do more of.

So far, this book has explained the many ways to remove your information from the internet. However, it is important to understand that it is not always possible to erase every piece of data about you. Disinformation will make that small amount of permanent data seem useless inside a stream of completely inaccurate content. I have devoted an entire chapter to disinformation techniques that I believe should be applied in some situations. This step is optional, and not suitable for everyone.

If you have been extremely successful with eliminating your online information, you may not need disinformation. However, if you have found a few services that refuse to remove your data, any websites that will not respond to your requests, or simply want to harden your overall security, disinformation may be the perfect solution. Providing inaccurate details while completing the removal processes discussed earlier will also increase your effectiveness substantially.

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 that you provide.

You have learned how public records, data brokers, advertising companies, and various businesses build complete profiles on you and your family. My main concern with these reports is the inclusion of my home address. Most people's home address can be found on 40 different websites within a minute. This is not only an invasion of privacy, but a danger to many people.

My goal with hiding from the internet was always to have a home that no one could associate with me. I wanted a safe location that I could feel comfortable in without looking over my shoulder. Police officers and other people targeted because of their profession will understand. After accomplishing this, I experienced an interesting moment.

In 2012, I received a piece of mail to my residence addressed to "New Resident". It was an automated welcome packet from several local businesses containing coupons for home related purchases. Basically, I had fallen so far off of the radar that data mining companies had assumed that someone else must have moved into my house. This was a rewarding feeling, but it quickly concerned me. If I was no longer likely to be living at my house, where did the data companies think I was living? I thought that too little information available about me could be causing more harm than good. This is when I became fascinated with disinformation.

A friend of mine is a private investigator. I had him lookup my information through a popular data broker that he had premium access with. There were no entries associated with me for the past few years. This indicates to an investigator that I was dead, homeless, or hiding. The only recent activity was my PO Box. I retained a copy of this report and used it as a comparison for future analysis.

The first call I made was to my internet service provider for my home. This was a major cable company and I started the conversation by requesting a discount

on my service. I was advised that if I extended my contract two years, I could negotiate a lower price. One of my arguments was that this was a second home and that I was hardly there. We agreed on a price, but I had two conditions. The first was that I wanted the bill and all associated records to be addressed to my full time residence. Second, I insisted that they only send me an electronic bill via email. This eliminated any need to have access to any physical mail coming from this company.

For my “full time residence”, I supplied an address that did not exist in a neighboring town. I went to Google Maps, identified a random nearby street, and found the last address available. I then added two digits to that address and attempted a search for it. Google identified it as a possible address, but it could not pinpoint exactly where the house was. I wanted to provide an address that would seem realistic, but not jeopardize anyone else. I never use any information that is unique and real to another individual. Another option would have been to identify a new neighborhood being built, locate the highest number for an address on the street, and add a few digits. If you are met with any resistance, you could say that it was a brand new house.

Within 30 days, I had my friend request another report on me. This time, it indicated that I had recently moved to an address that matched the disinformation that I provided to the cable company. I considered this a success and continued with my disinformation campaign.

The remaining content of this chapter will identify possibilities that you may consider for your own disinformation attempts. They are divided into three 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.

Name Disinformation

In the perfect scenario of hiding from the internet, every reader will be moving soon, can purchase the home in cash, possesses an invisible New Mexico LLC for the title, and will never associate the new address with a real name. In order to be realistic, I will assume this is not the case for you. 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 increase your privacy quickly. At the end of this section, I will display actual results from these techniques.

Bills

Earlier, I explained how to use disinformation to have a landline telephone listing modified to inaccurate information. This technique works well on practically any service provided to a home or business. Contact the service provider, possibly your cellular telephone provider, and request a change to your billing information. Advise the representative that the account is listed under your middle name and that you are uncomfortable with that and desire it to be associated with you first name. Provide any first name that you like. Within weeks, third party companies will receive the updated information which will eventually override the real information on file. I prefer to choose a different first name for every bill.

Magazines

If you have a subscription to any magazines in your real name, you should stop that practice immediately. This data is openly shared with many companies and will quickly identify your name and home address online. Contact the magazine

company and tell them that you were recently married and want the magazines delivered in your married name. Provide any last name that you desire, as long as it has no personal association with you. This works for men as well. Since same sex marriage has been so controversial lately, no magazine company is likely to challenge a man on changing his last name to his partner's.

If you do not have any magazines delivered to your home, it may be time to start. Identify a couple of popular magazines that 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. This will often involve the need to complete a short survey. The survey can also be used as a disinformation opportunity.

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 that 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.

Newspapers

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 that will allow 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.

Trade Mailings

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 that live at your home. I would only choose this option if you do not take advantage of a magazine or newspaper subscription.

House Repair

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.

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 living trust. Instead of providing the full name of the trust, leave off the description at the end. If your trust was titled The Big Adventure Revocable Living Trust, you could use The Big Adventure Contracting Company.

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. If you have an LLC or a trust, consider opening a free checking account in the name of it. This will not only add a layer of anonymity, but it will also enforce the appearance of legitimacy.

Name Disinformation Results

A friend allowed me to conduct various forms of disinformation on his home address. Before I took any action, I performed a basic search on Spokeo for his address. It provided one result, which positively identified his name, address, telephone number, email address, and family member's names. At the completion of my disinformation campaign, I allowed 60 days to pass. The new result identified 80 unique people that live at his address. Much of this is due to the methods that will be discussed in the following sections.

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.

Choosing an Address

This section will explain how to create at least three valid addresses that you will 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 that is discussed earlier as possible 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. This is my favorite technique. 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 that displays new homes for sale. The newly planted grass, identical houses, and same list price in each listing are also an indicator 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 digits. 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 that 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.

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.

Internet Surveys

There will never be a shortage of internet surveys. These are websites that ask you to answer numerous personal questions and offer small rewards in return. Most of them never fulfill their promise to send you money, tech devices, or Amazon gift certificates. They all collect your information, create large databases of personal details, and sell that data to marketing companies. The content associated to you often makes its way to the public visible internet.

These surveys are time consuming but effective. The content that you provide will quickly be disseminated to various public sources. Be sure to always provide your real name, but never provide your real address, personal email account, or any real information about you within the survey responses. You do not want to create an accurate profile of your interests and family situation.

Many readers will want nothing to do with this section. I completely understand this stance, especially when seeing the level of intrusive questioning that is involved. I only recommend this approach when you have been unsuccessful at removing your personal details from the internet such as the city and state you live in, your age, and family members' information.

In order to explain the appropriate way to provide disinformation through online surveys, I will demonstrate using swagbucks.com. The following instructions will walk you through the process.

- ✓ Navigate to swagbucks.com and create a new account. Provide a 33 Mail address created earlier and a password used only for that website. I recommend using a specific 33 Mail account such as swagbucks@nsa.33mail.com. Be sure to use a 33 Mail account that will forward to you. You will need to verify this email address by clicking the option within an email sent to your 33 Mail account.

- ✓ You will be given the option to "Complete Your Profile" in a popup window after email verification. Choose this option and provide your real name. This website will walk you through providing your gender, date of birth, zip code, and other personal details. Provide inaccurate responses to all of these. Within weeks, this false information will start to appear within public people search sites.

- ✓ Complete a few surveys always providing inaccurate answers. You will be prompted to complete a "Profiler" which will ask many invasive questions related to income, race, employment, education, health issues, and sexual orientation. Always provide inaccurate data. Three to five surveys should be enough to pass your name, false age, and incorrect location details to third party companies.

TV Offers

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 any situation that you are in. 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 of 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.

Online Offers

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 listed in several marketing databases quickly with this false information.

Home Scooter

Time Share
Home Alarm
Lawn Treatment Service
Home Food Delivery

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. 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.

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.

Social Networks

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 that 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 of 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. If this type of disinformation is appropriate for you, it can

be taken further with the following technique.

GPS Spoofing

Most social networks allow you to share your current location at all times with the world publicly. The readers of this book will likely think that this is ridiculous. While I agree, we can also use it to our advantage. Manipulating the location information stored within social network posts can be very easy or fairly difficult. I will explain two different options to consider based on your level of technical skill.

Please Don't Stalk Me (pleasedontstalkme.com)

The easiest way to spoof your location on Twitter is to use the service Please Don't Stalk Me. This website will perform all of the necessary actions in order to provide a false location during your "Tweets". The following instructions will explain the process.

- ✓ Either create a new Twitter account or log into your current Twitter account from which you want to post messages. Confirm that you have location sharing enabled by going to Settings > Security and privacy > Tweet Location. You want to check the box that allows you to add location information to your Twitter posts.

- ✓ Navigate to pleasedontstalkme.com and allow it to connect to your Twitter profile through the "Sign in with Twitter" button.

- ✓ Enter the address or general location from which you want to appear to be posting your message. Click the "Tweet" button to post the message.

- ✓ Navigate to your Twitter profile to view the post and associated location information. The upper right marker and location confirm that the message was posted from New York City while I was really sitting in Chicago.

- ✓ If you want to test the accuracy of your false GPS information, load your profile on the website tweetpaths.com by entering your Twitter user name.

Providing false location information to your Twitter posts can be extremely effective for disinformation purposes. While I usually encourage people to stay away from social networks, this can be helpful. If you are trying to convince an abusive ex that you now live in a new area, frequent posts with false location data from that area can be very convincing. If you want your family and friends to believe that you are vacationing overseas, this technique should fool them and allow you some peace and quiet in your own home.

Please use caution not to divulge any accurate personal details. Always remember that the content that you post to the Twitter servers will likely be present forever and can never be completely removed.

Web Browser GPS Data

The previous technique is great if you only need to fool someone through Twitter. It does not work for other services. We can emulate a GPS location within our web browser and allow the browser to share this with any website. This will cause social networks to broadcast our current location, which we can control with misleading information. This can quickly confuse anyone that is stalking or harassing you. The following instructions will walk you through the entire process of providing false location data to a Twitter profile and posts.

- ✓ Download and install the Chrome web browser. This free browser works on all operating systems and will often provide a faster internet browsing experience. Navigate to google.com/chrome and follow the directions.

- ✓ Launch Chrome, click the menu in the upper right corner, highlight “More Tools” and select “Developer Tools”. This will launch a new window on the side of your screen. Strike the “ESC” key on your keyboard which will launch the necessary console at the bottom right. Click the word “Emulation”, then “Enable Emulation”. Click

"Sensors" on the left menu of this window. Select the "Emulate geolocation coordinates" checkbox and enter any GPS location that you desire.

- ✓ Close the developer tools console by clicking the "X" in the upper right corner of the tools box at the bottom of your screen. You should now only see the web browser page.

- ✓ Navigate to Bing Maps (bing.com/maps) and click the icon next to "Click to center the map on your current location". Your browser will likely ask you if you want to share your location. Accept this request and the map should identify that you are at the location that you provided.

- ✓ Connect to any network that you want to use to broadcast a false location. You should connect to the mobile versions of the services you want to fool. Instead of facebook.com, you should connect to m.facebook.com. Adding "m." or "mobile." in front of most websites will take you to the mobile version which will ask for location information.

Be aware that this technique does not hide or change your IP address. Websites that you visit will still know this information and may be able to determine your approximate real location. This should only be used for purposely posting false location data through social networks. Always test this procedure with a non-sensitive account to validate the result.

Address Disinformation Results

I consulted a government employee that was being harassed by a federal prisoner that he had arrested. The prisoner threatened to find his family and kill them in their sleep when he was released from prison. With permission, I began a disinformation campaign for him. He had a unique name and lived in Chicago. Before the process, searching his name in Spokeo identified two locations. One was his home and the other was his workplace. After removing these entries, which was discussed earlier, I helped populate false information through the

techniques discussed here. The current result when searching his name displays over 20 possible addresses, and none of them relate to his actual home.

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.

Identifying New Numbers

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.

Busy Numbers

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 this area and the numbers should not be assigned to any customers. Since these are not toll free numbers, they should not be flagged as non-residential. Because numbers are ported so often, possessing a number in another area code should not raise any suspicion. When you give someone a number that is always busy, it does not create the appearance of a fake number. These may appear real to a person that would otherwise question the validity of a given number.

Disconnected Numbers

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.

717-980-0000 through 717-980-9999

Always test the numbers that you choose before using. The following table displays a useful chart of the “busy” numbers with an area next to each to document the numbers used and specific application of each. You could use this to keep track of your disinformation.

909-661-0001	_____	909-661-0031	_____	909-661-0061	_____
909-661-0002	_____	909-661-0032	_____	909-661-0062	_____
909-661-0003	_____	909-661-0033	_____	909-661-0063	_____
909-661-0004	_____	909-661-0034	_____	909-661-0064	_____
909-661-0005	_____	909-661-0035	_____	909-661-0065	_____
909-661-0006	_____	909-661-0036	_____	909-661-0066	_____
909-661-0007	_____	909-661-0037	_____	909-661-0067	_____
909-661-0008	_____	909-661-0038	_____	909-661-0068	_____
909-661-0009	_____	909-661-0039	_____	909-661-0069	_____
909-661-0010	_____	909-661-0040	_____	909-661-0070	_____
909-661-0011	_____	909-661-0041	_____	909-661-0071	_____
909-661-0012	_____	909-661-0042	_____	909-661-0072	_____
909-661-0013	_____	909-661-0043	_____	909-661-0073	_____
909-661-0014	_____	909-661-0044	_____	909-661-0074	_____
909-661-0015	_____	909-661-0045	_____	909-661-0075	_____
909-661-0016	_____	909-661-0046	_____	909-661-0076	_____
909-661-0017	_____	909-661-0047	_____	909-661-0077	_____
909-661-0018	_____	909-661-0048	_____	909-661-0078	_____
909-661-0019	_____	909-661-0049	_____	909-661-0079	_____
909-661-0020	_____	909-661-0050	_____	909-661-0080	_____
909-661-0021	_____	909-661-0051	_____	909-661-0081	_____
909-661-0022	_____	909-661-0052	_____	909-661-0082	_____
909-661-0023	_____	909-661-0053	_____	909-661-0083	_____
909-661-0024	_____	909-661-0054	_____	909-661-0084	_____
909-661-0025	_____	909-661-0055	_____	909-661-0085	_____
909-661-0026	_____	909-661-0056	_____	909-661-0086	_____
909-661-0027	_____	909-661-0057	_____	909-661-0087	_____
909-661-0028	_____	909-661-0058	_____	909-661-0088	_____
909-661-0029	_____	909-661-0059	_____	909-661-0089	_____
909-661-0030	_____	909-661-0060	_____	909-661-0090	_____

Store Giveaways

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.

This content 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 listed previously. 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.

Shopping Cards

Most grocery stores have a shopper’s card program that 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 of the items that you purchase. The risk of joining is the guaranteed profile that will be created about you and sold to interested parties. You can enjoy the benefits without jeopardizing your privacy. This is a great opportunity for telephone number disinformation.

Practically all of the stores that 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 following telephone number to work at most stores.

867-5309

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.

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 at my 33 Mail account. I will never use that email account again, and will know which company provided my information when I receive unwanted email at Safeway@nsa.33mail.com. I can now provide 847-867-5309 as my member number when I shop at Safeway. Most importantly, you can too.

As a community service, I create new accounts at every store that I can in 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 legitimate information difficult to find and harder to prove accurate.

Rewards Cards

Chapter Five discussed a method of using hotel reward programs to help convince a receptionist to accept your credit card in your alternate name. These programs can also be used to spread disinformation for your benefit. Many companies that offer reward programs share or sell the collected data to other interested businesses. If you have an account with a chain of luxury resorts, they are likely to sell your information to credit cards that cater to business travelers. If you are a rewards member of a fast food chain, they are likely to share your

details with other food and retail companies. While some privacy advocates warn you to stay away from these traps, I encourage you to embrace them with disinformation.

Rental Vehicles

I travel often and find myself in a rented vehicle monthly. I joined various rewards programs in order to obtain substantial discounts and upgrades. I always provided my real name because a driver's license was always required to complete a transaction. However, the address and telephone number was never verified during the signup process. Every time that I would rent a vehicle, I was asked if I was a rewards member. I always advised yes, but stated that I did not know my membership number. The most common response was "What is your telephone number?".

Like many other programs, most car rental rewards clubs can access your account by telephone number. The telephone number is heavily associated with your name and a great opportunity to provide disinformation. The details that you provide will likely become visible either publicly or to data marketing companies. Providing your real name, disinformation address, and one of the telephone numbers discussed earlier will help create an inaccurate profile and may help eliminate your real telephone number that is currently on file with other companies.

You do not need to actually use any of the services that you register with. All of them allow you to join their rewards program before you make any reservations or purchases. The information below will take you directly to the online application process for some of the popular vehicle rental companies.

Enterprise: enterprise.com/car_rental/enterprisePlusCreateAccount.do
Hertz: hertz.com/rentacar/member/enrollment/contact-details
Thrifty: thrifty.com/BlueChip/Enrollment.aspx
National: nationalcar.com/index.do?action=emcIndex.do&type=uszl-withnav-header
E-Z Rentals: e-zrentacar.com/rewards/money_main

Caller ID Apps

Mobile apps such as TrueCaller were discussed earlier. They collect the contacts from your device and add them to a huge database that anyone can search. You can use this to your advantage. If you have an unused smart device, conduct a hard reset to remove all personal data. Connect to Wi-Fi and add your real telephone number to your contacts but provide a random name. Install every caller ID app that you can find and agree to the permissions. This will identify your real number as someone else's. If someone searches your number on the website, they will receive a result with a random name. While not always foolproof, this can add a small layer of disinformation to your overall strategy. This could be completed for every VOIP number that you use. You could also provide disinformation for your family's numbers without them knowing. Maybe your child needs this assistance.

Phone Number Disinformation Results

A college student of mine once told me that her ex-boyfriend was constantly harassing her through telephone calls and text messages. She had changed her number once, but he was eventually able to find the new number through the internet. With her permission and assistance, I embarked on a telephone disinformation campaign before she changed her number again. Eventually, Spokeo and other services associated her name with three of the "busy" numbers, her email address with a 33 Mail account, and her home address with a non-existing building. She was now ready to change her number for the last time, and keep it out of any public databases.

General Tips

- ✓ Consider always providing disinformation that will help you identify the leak of data when you find it. For example, if you request information from a reverse mortgage company with a goal of name disinformation, you should use a name that will remind you of this company, such as "Joe Reversi". When you receive unwanted mail at your residence attached to this name, you will know the original source.

- ✓ A benefit of disinformation involving companies that cater to a specific demographic is that your residence will now be associated with the same category. Requesting reverse mortgage information or a medical alert quote will likely indicate that older adults live at your residence. This can help mask your real interests.

- ✓ Never use your real name or alternative credit card name in association with your real address or telephone number. The goal here is to generate inaccurate details in order to help mask any real data that you cannot remove.

- ✓ Remember that it will be difficult to remove disinformation that you provide about yourself. If you have very little online information identifying your personal details, these techniques may not be appropriate for you. However, if there is an abundance of accurate details that you cannot remove, it is better to add bad information in order to hide the real content.

You may desire a written reference for your disinformation campaign. The following page includes an area where you can document your details for later use. This includes three sections. The name disinformation area should include your real address, but no other factual information. The address disinformation should include your real name, but no other factual details. Finally, the telephone disinformation section should include your real name, but not a telephone number or address registered in that name. This page may be helpful as reference when executing your own disinformation strategy.

Name Disinformation:

Alias Name # 1 _____

Alias Name # 2 _____

Real Home Address: _____

Alias Telephone: _____

Address Disinformation:

Real Name: _____

Alias Address #1: _____

Alias Address #2: _____

Alias Telephone: _____

Telephone Disinformation:

Real Name: _____

Alias Address #1: _____

Alias Address #2: _____

Alias Telephone #1: _____

Alias Telephone #2: _____

Alias Telephone #3: _____

Chapter Thirteen

Aliases

I have mentioned legally using a secondary credit card under an alias name several times in this book. This is used in situations when disclosing your true identity is not necessary. We should now take a look at selecting an appropriate alias name and corresponding details related to this new identity. For some, this may be a simple and random thought. Some may pick John Williams as their new alias. I prefer to make an effort to intentionally choose proper details that have been thoroughly reviewed for long term use.

The most vital lesson in this chapter is to be prepared. I never “go live” with an alias name without having all information in place. This may include your alias address, phone number, email address, middle name, mother’s maiden name, and other details. I have been caught off guard in these situations. I recently helped someone order anonymous internet access to their home and was asked for my email address for the automatic billing. I had not created one yet. It became awkward when I had to say “hold on” while I quickly created one. Instead, be prepared for everything. Hopefully, this chapter will help you in these preparations.

In Chapter Three, I discussed preparation for your journey into removing your details from the internet. The material focused on having anonymous email addresses and phone numbers to give out. These would be associated with your real identity in an effort to protect your private information. This chapter is much different. None of the previous work should be used here. This chapter will help you create new content that will never be associated to your real identity. It will be attached to your alias identity only.

Choosing your alias name, sometimes referred to as an alternative or secondary

name, is very important. You need to be comfortable with it. You need to respond to it when called in a crowded room. Basically, it needs to be natural. I do not promote obvious names such as John Williams or Jane Smith. These sound fake. This might bring more attention than desired. Instead, consider a new version of your current name.

If you have a common first name, such as Michael, I do not see much risk in keeping that first name. Instead of Michael Bazzell, you may create a secondary identity of Michael Williams or Mike Wilson. This maintains the natural response to people calling you by your first name. The unintentional nuances that you exhibit in relation to your true identity are difficult to replicate when using a new first name. People that enter the world of covert government work may be prepared to take on a completely new identity. Most of my clients are not ready for that task. Before I can get into the details, I need to discuss things you should never do.

- ✓ Never choose an alias name of someone that you know.
- ✓ Never choose an alias name with the intent of portraying another real person.
- ✓ Never use an alias when identifying yourself to a government official, especially any law enforcement. That is a crime.
- ✓ Never attempt to obtain any credit under an alias name.

Some clients, especially female victims of domestic violence, desire a completely new name. They do not want to recycle their first name and want a fresh start. I completely understand this and encourage you to do what is best for your situation. The most difficult part of selecting an entire new name is ensuring that it has no ties to you. While it may sound easy to pick a random name, try it for yourself. As you read this, mentally state your new alias without giving it much thought. The name that you just chose likely fits into one of the following categories. If it does, it should not be used.

- ✓ The full name of a famous person.

- ✓ The first name of a relative or friend.
- ✓ The last name of a fictional movie or television character.
- ✓ The middle name of a close ancestor.

This list could go on, but you get the point. We tend to pick names that have some type of meaning to us. This is bad because it might leave a trail to your real identity. I suggest you come up with names that have no relationship with your past. As of this writing, the ten most common last names in America are the following.

Smith	Williams	Jones	Davis	Rodriguez
Johnson	Brown	Miller	Garcia	Wilson

I believe that these make for great last names. They are vague enough to be difficult to search, and popular enough to appear legitimate. If you use a common last name, I suggest using a slightly more unique first name. Remember that names like Jane Smith seem fake while Alicia Smith appear to be a bit more authentic. Only you can create the alias best for your situation. I only ask for you to consider these recommendations.

After you have selected the new alias name that you will use, you need to create the digital life that will go with it. At the minimum, you need a new email address and telephone number. If you want to truly be prepared, you will also need an alias mailing address, employer, hometown, social networks, credit card, identification card, family history, and digital footprint. I will explain each in its own section below.

Email Address: This is vital. You need an email address that you can give out at any time that can be associated with your new alias. I believe that the address should include your alias name within it in order to appear more legitimate. If your alias name is Brad O'Neal, and your email address is robert911@hotmail.com, this seems suspicious. If your address is brad.oneal.5@outlook.com, this appears more authentic. The host of your email

address is not very important. If you plan on incorporating a Google Voice number into this alias, it may make most sense to create a Gmail address. While I dislike Gmail's intrusive collection of your personal information within your emails, I will accept it for this purpose only. None of your communications will be associated with your real identity. You will also delete all messages in a timely manner.

Telephone Number: I believe that this is also vital. You will need a number to give businesses when you use your alias. This number should connect to a generic voicemail that you have access to. A Google Voice account will suffice for all of this. Forwarding your voicemail messages to your 33 Mail account will make sure that you have immediate access to these messages within your personal email account (non-Gmail). Chapter Three explains everything you need to know about creating Google Voice accounts.

Employer: You should always have an alias profession memorized and ready to deliver. Our society really enjoys small talk. When meeting people for the first time, you will likely be asked within a couple of minutes about your profession. Some are truly interested in what you do, but most are trying to appear polite because silence feels awkward. When choosing your alias profession, be careful not to violate any laws. Never state you are a police officer or a federal agent. This is a crime. It is also a crime in some states to identify yourself as a coroner, judge, paramedic, or other government employee. I highly recommend to stay away from anything close to this. I also suggest that you avoid professions that you know nothing about. Imagine that you just told the clerk at the hotel that you were a truck driver. She then tells you that her father is a truck driver and asks about your rig. You are now stuck in this lie and are on the spot. Instead, consider keeping things generic. I prefer to state I am a self employed consultant, tech support, or data entry employee. This is usually boring enough to stop further questioning. I never recommend stating something too interesting. If you tell the people at the table of the conference you are attending that you are a pilot, you will now be the focus of attention.

Hometown: Similar to questioning your employment, people tend to ask "Where are you from?". If you are from a small town, and disclose this, you might be disclosing too much information. I prefer to state that I am from a large city that I know something about. If I say I am from Chicago, the next question

will be “What part?”. You had better be prepared. I like to pick a well-known landmark in a residential area and use that. I have a client that tells everyone he is from Chicago. When pushed for more data, he states “Two blocks from Wrigley Field! Do you like the Cubs?”. This then puts the questioner in the spotlight and allows him or her to talk about themselves. This usually results in a topic change very quickly.

Social Networks: In Chapter Nine I encouraged you to minimize or delete your social networks. In contrast, I now suggest that you create some. If you are going to use an alias name with people that you might continue a relationship with, you should probably have an online presence. This does not mean that you should create profiles on ten different networks, but you should have at least two. I recommend a Facebook profile and Twitter account in your new alias name. This way, when someone tries to check up on you, there is something to see. Keep the alias personal data minimal, set your privacy settings appropriately, and occasionally post extremely generic information. On my accounts, I occasionally retweet a celebrities’ comments on Twitter or respond to random people on Facebook when they post their birthday. I post just enough to seem real without divulging any real information.

Credit Card: Chapter Five explained how to obtain a secondary credit card in an alias name. If you plan on using this name in front of other people while dining, shopping, or making any purchases with a credit card, you should be prepared to pay with the proper card in that name.

Identification Card: This gets tricky. I do not want to commit any crimes, but I may need photo identification at some point. I had a client that attended an invite-only party at a popular club. The person that invited her knew her as the alias name that she had provided on an attendance roster during a public event. At the time, she did not want to give out her real name because it was an event surrounding a controversial subject. Entrance to this party required photo ID. Fortunately, she was prepared. In her wallet with the secondary credit card, she possessed her gym membership card. Since she had registered for her gym in her alias name, and she pre-paid her monthly dues with her secondary card, they never asked for identification. They created her membership card for her after taking her photo with a digital camera. At this new event, she displayed her gym membership card to the bouncer stating “I left my DL at the gym, but you are

welcome to call them to verify that". The bouncer matched her alias gym membership name to the name on the list and waived her through. She committed no crimes during this process. It is important to discuss again the importance of staying legal. Never create an identification card that appears similar to any government ID and never give an alias to any law enforcement. I will later discuss alternative ways to obtain identification in the name of an alias.

Family History: The people that ask you about your hometown and profession are likely to also inquire about your family history. Questions such as "Do you have kids?", "Do your parents still live in Chicago?", and "Do you come from a big family?" are very common. I recommend that you are prepared for this. In many situations, you might want be honest in order to remember what you have disclosed. However, this often leads to more questioning. If you say that you are from a big family, you will likely be asked if you had brothers or sisters, if you are the oldest, where they all live, and other details. This may make you uncomfortable when talking with strangers who are only trying to be polite. Ultimately, you should choose the best option for you and stick with it. I prefer minimal details. Therefore, I usually stick with simple answers followed by a question such as "I was an only child, what about you?".

Digital Footprint: This is an area that is often overlooked by privacy seekers. We tend to stop ourselves from sharing anything on the internet. However, your alias is not you. Think of him or her as the exact opposite as you. Your alias may be a social maniac that desires online fame. This can help establish your alias as a real person and really "sell" it. If you want to build up the persona of your alias online, I recommend that you consider the following avenues.

Practically everyone has a blog or media website today. We cannot generate enough content to keep up with the demand of new material. Therefore, practically every outlet accepts guest posts from readers. If you follow a blog about finance, you could likely write an article and have it posted under the name of your alias. If you have an interest in technology, there are numerous websites that will publish your original article without much scrutiny. I believe that this method establishes better credibility than a social network profile. While anyone can create either anonymously, the published content appears more legitimate. Consider the following true scenario.

A client had established an alias name, email address, and social networks. He planned to use this alias while interacting with a local hackerspace. While most hackerspaces understand your desire for privacy, this one asks that you disclose your real name when interacting with members. He was uncomfortable with this because of the unfortunate negative connotations surrounding hackers and hackerspaces. He also held a respectable position at a law firm and did not want to associate his professional life with his personal interests. He has also observed the hackerspace website disclose the real names of the people that attended past events. He knew that the group would likely Google him at some point and he wanted to appear legitimate.

He sent an email to over a dozen of his favorite technology related websites asking if he could write an article explaining the details of his classic arcade machine project using the M.A.M.E arcade emulator and a Raspberry Pi device inside a refurbished arcade cabinet. Three responded right away and were happy to publish his work. He sent the well written article to all three, disclosing that he would be posting on multiple sites, and waited. A few days later, his article appeared on all three websites in the name of his alias as the author. All three were linked to his alias Twitter account in order to contact the author. If you Google his alias name today, the first two results are links to these articles. This not only helps his alias appear real, but it also declares that his knowledge coincides with membership into the hackerspace community. For those wondering, he approved this disclosure here and encourages you to try to locate his true identity.

For most people, possessing a single alias is sufficient. It gives you an alternate name to use when appropriate to protect your privacy. It is enough to get you out of awkward situations. If you are well prepared and have adapted to your alias details, the information you provide will sound smooth and authentic. I encounter situations every day that support the use of aliases. Consider the following scenario.

A large national chain of hair cutting services offers affordable cuts to a mostly male audience. When you arrive, they ask if it is your first visit. If it is, they ask for your first and last name, home address, and cellular telephone number. This is for marketing purposes and to text you when it is your turn. They then ask for your date of birth in order to give you a free cut on your birthday. They ask for

identification if you want to take advantage of this. The data is searched based on the telephone number. If it is not your first visit, they will ask for your number in order to retrieve your visit history and access your data.

I recently visited this chain while traveling during speaking engagements. While desperate for a haircut, it was the only option on a Sunday afternoon. When prompted for this information, only a first name of John was given. The statement “I prefer to pay with cash and decline to offer any personal information” was given during all other questioning. It was a bit awkward, but worth the hassle.

Many people might scoff and say “who cares if your barber knows this information?”. I do, and you should. It is not a matter of an individual knowing your birthday. Instead, it is a matter of you protecting your personal data and privacy. When you hear about that service announcing a breach of all of their customer data, you will not be concerned. When the company sells their customer database to a data mining company for a few thousand dollars, your name and home address will not appear on the internet. The small actions that we take to prevent the leakage of our personal information will have a huge impact on our overall privacy. Everything is connected.

Some people require multiple aliases. I only recommend this to those that can keep all of the details straight and have a need for additional names. Before I explain my recommendations, you should understand the scenarios when one alias is not enough. Consider the following example that was sent to me via email after reading the second edition of this book, shared with permission from the sender.

A woman was the victim of constant harassment from a former lover. He was mentally and physically abusive and a drug addict. On several occasions, she would leave their shared apartment and stay in a hotel for safety. He would call all of the hotels in the area and convinced hotel staff that there was an emergency. Through social engineering, he was able to identify her hotel room number. This created a very dangerous situation.

She finally left him permanently and moved into a new apartment in another portion of the city. She attended numerous local conferences as part of her job

and often stayed overnight in the hotel that was hosting the event. She created an alias to use during these travels in order to hide from any future attempts. This worked great for a while.

She used her new alias every time that she checked into a hotel. She also used the same alias with her new book club that she joined. Eventually, the former boyfriend went to every book club meeting held at independent book stores in the area. He knew that she enjoyed these and thought he would find her eventually. When he spotted her, he likely watched from a distance. When she left the book store, he approached the remaining members and turned on his charm. He gave the following story to one of the elderly members of the club.

“I am so sorry to bother you. I have a weird story to share, and you might think I am crazy. You see, I am a true romantic, almost to a fault. I met a woman the other day here at the store, and I will never forgive myself if I do not try to contact her again. We had so much in common, and she was so beautiful that I could not build up the courage to ask her out. I only know what she looks like, and I do not even know her name. She mentioned that she belongs to this book club, but I guess I arrived here too late. Do you by any chance know who I am talking about?”

Immediately, the woman screamed “I bet you mean Amy!”. The other ladies then joined the conversation and were determined to get these two together. He left there knowing her first and last alias name, the area of her new apartment, the current book she was reading, and the details that she shared with the group about her ex (him). The harassment began right away.

I believe that readers that are in any type of physical danger should have two aliases at a minimum. One of these should be used solely during travel. It should be used at hotels and while shopping. It should not be used in any type of social gatherings or personal environments. “Amy” should have a personal alias and travel alias. They should be different first and last names and should have no obvious connection to each other. Your situation may require a third or fourth alias, but that is very rare.

Isolating these aliases within their own wallets are vital. 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 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.

I support isolating your alias documentation in individual collections that are similar to each other but uniquely identifiable. One client found an online store that sells a “Slim Wallet”. It is a bi-fold leather wallet that will hold a small amount of cash and up to four cards. It is available in several colors. He keeps three wallets in his backpack at all times. One color is his true identity with real driver’s license 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. The black wallet is his primary alias that he uses for generic occasions. This contains a secondary credit card in his alias name which he uses for shopping, dining, and social interactions. It also contains his gym membership card and random frequent visitor food reward cards. They are all in the primary alias name. The final wallet is red and only used during travel. It contains another secondary credit card and several hotel rewards cards, all in his alias name.

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, and a $2 bill covers the fourth.

You may be struggling to think of ways that you can possess identification cards in your alias name legally. I offer the following as theoretical options. Be sure to check all state and federal laws before attempting any of the following.

- ✓ Practically every hotel chain offers an online enrollment into their rewards system. This will present you with a plastic card in any name you desire. While no photo is on these, it helps create the illusion of a real person. It provides “padding” to your wallet to convince others.

- ✓ Many volunteer programs insist that you wear identification while providing your services. Zoos, museums, gardens, libraries, and attractions often have volunteer groups that provide tours, guidance, or post event trash pickup. Some of these issue photo identification to be worn around a lanyard to identify you as an authorized visitor. If you are not being paid, very few of these verify your identity. With this method, you can establish an alias, obtain an unofficial photo ID, and give back to your community all in one step. Be careful not to violate laws surrounding your access. If you are a registered sex offender required to stay away from schools, an alias does not circumvent this to allow you to help after a school event. You will get caught and arrested.

- ✓ Many travel groups issue identification cards to be used while on tours of a city. These are also usually worn around your neck in order to identify yourself as associated with that tour. I have seen city tour gatherings leading groups of people around major cities. All of them have a similar laminated card on a lanyard with their photo and name, along with the name of the tour group.

- ✓ Many large corporations provide occasional tours of their campus. In years past, this meant that you showed up and followed a line of people while learning about the features of the product made by the company. Today, you are often required to wear a visitor's pass. Many corporations now collect a digital image of each visitor and print this image on a paper label to be worn on clothing. While many of you will cringe at the thought of providing a photo of your face, I do not get too bothered by this. We are all already being monitored on CCTV. You could attend a tour, provide an alias name, and receive a business card sized label that includes your alias name, company logo, and real photo. An affordable laminator can quickly give this the appearance of legitimate identification.

One final option is to simply make your own. I hesitate to discuss this option too much in detail because people may try to break the law and create fake government ID's. 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 ID's online, but most are illegal. Instead of presenting you with random ideas, I prefer to separate legal and non-legal options.

- ✓ **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.

Aliases possess an unfair view 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 true identity 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. I ask you to consider scenarios where using an alias name might protect you, your family, and your identity.

The following page possesses a worksheet to be used later for reference. It is a place that you can document your alias information. It may be useful during telephone calls or online orders. I always recommend being prepared when using an alias. Having the information in front of you can never hurt.

Alias Name: _____

Alias Home Address: _____

Alias Home Telephone: _____

Alias Cellular Telephone: _____

Alias Email Address: _____

Alias DOB: _____

Alias Employer: _____

Alias Employer Address: _____

Alias Hometown: _____

Alias User Name: _____

Alias Credit Card: _____

Alias Family History: _____

Alias High School: _____

Alias College: _____

Alias Sports Interests: _____

Alias Music Interests: _____

Alias Misc. Hobbies: _____

Chapter Fourteen

Future Habits

By now, you have learned how to hide from public searches on the internet. If you have applied the techniques, it will also be difficult for private investigators, attorneys, and marketing companies to find you. This success can be quickly ruined by repopulating your personal information into public view. Preventing new data from being collected about you is as important as removing your personal information. The way that you previously provided your personal details to others must change immediately.

In this chapter, I have provided the most common scenarios that will jeopardize your privacy. Reacting to these the wrong way will introduce your personal information back into the public. In each scenario, I have outlined the appropriate way of responding to the situation in order to protect your personal details. I hope that you use this chapter as a reference when you need some ideas on how to stop people and companies from intruding into your life.

From this point onward, you should never associate your home address with your name or the names of your family members. At first, this may sound difficult to do. To help with the transition, continue reading. There will be exceptions, which will be explained later. Overall, I believe that your personal information, such as real name and home address, falls into two categories: public and private. If there is any chance that your details will be shared with other companies, you should not give your information to that entity. It may be easier to identify the situations that warrant disclosing your real name, date of birth, and SSN. These are few and include items such as Financial Accounts, Employer Tax Forms, Medical Records, IRS Tax Filing, Airfare Purchases, and Passport Documents.

None of these require your home address. All will accept a PO Box legally. Your employer may have policies demanding a physical address. I will present ideas on this later.

Age and Identity Verification

There will be times when you are “carded” in order to verify a minimum age. This may be at the grocery store when you purchase alcoholic beverages or to gain access to an “over 21” area at an event. For most situations, I do not mind displaying my driver’s license. The employee is only looking at your birth date and no information is being collected into a system. This is not always the case. Recently, I attended an event at a local casino. Upon entry, everyone had to show identification for age verification. If you frequent the casino often, the player’s card will escalate you through this process. Since I do not participate in these programs, I was stuck in line. I watched my friend ahead of me display his license which was scanned into a card reader by a gaming agent. The computer displayed my friend’s driver’s license photo and information. I had no doubt that his information had just been added to this chain of casino’s database. He was allowed to pass. As my paranoia kicked in, I pretended to receive a cellular call and got out of line to retrieve a forgotten item from my car. When I returned, I walked through the line without showing my license and personal address. How did I do it? I displayed my passport.

Passports are accepted practically everywhere as proof of identity. They contain your name, date of birth, and a photograph. A passport contains a unique number assigned to you that can be used in place of a driver’s license number. This number is much more difficult to trace by the private sector. A passport has never contained a home address.

I contacted my friend a few months later and inquired about the casino. I asked if he ever receives advertisements and offers from them. He replied that he gets coupons and announcements from them in the mail. After thinking for a moment, he said that he also gets mailings from other casinos owned by the same company. He verified that he had never signed up for anything through the casino. They must have used the data from his driver’s license. I suspect that the data collected will eventually find its way to a company that will not keep it private.

Any time you need to provide proof of your name or age, consider showing your passport. While it can be scanned in the same manner as a license, very few establishments have the hardware devices to do this. Banks, hospitals, airports, and hotels are familiar with passports and should never offer resistance in their use.

Post Office Box Issues

There are occasions when companies will refuse a post office box as a mailing address. This has nothing to do with the deliverability of mail to the address. They just want your home address to add to your profile. Therefore, they have rules in place that will reject your box number in an online form submission. The only times that a physical house address must be verified are when you are establishing a new line of credit or completing official government paperwork. Any other company should only receive your post office box address. There is a way to usually force it.

Assume that your address is PO Box 9985, Chicago, IL 60601. There must only be one box with that number in that zip code. When your online form refuses to accept your address, enter it in reverse order. Enter it as 9985 Box, Chicago, IL 60601. The post office will know that any mailings to this address should be sent to your box. This format should meet any requirements in an online form. You may notice that some generic advertisements are addressed in this reverse format.

Outgoing Telephone Calls

When you make a telephone call, the receiver can identify you by your caller identification (caller ID). Since this is common knowledge, many people dial “*67” before the telephone number to hide their identity. This causes the caller ID display on the receiving end to display “Unknown Caller” or “Blocked Call”. This does not work at large companies. If you attempt to block your caller ID when calling a toll free number, your details will not be blocked. Large companies have telephone systems that will still display your name and number regardless of masking attempts. Because of this, you should be careful when calling large businesses. If you call from your landline telephone, your information will automatically be populated into the company’s database. You

will now be more susceptible to receiving calls from the organization. If you call from your cellular number, your number will be collected, but not your name. When you discuss your account with the business, your number will be added to your customer profile. If this concerns you, consider these alternatives.

- ✓ Place the call from a pre-paid cellular telephone.
- ✓ Place the call through a VOIP service such as Google Voice (free).
- ✓ Contact customer service through internet services such as email or website chat.
- ✓ Request a call from the company to your anonymous number through an email message.

Vehicle Servicing

Having your vehicle serviced will usually result in your information entering advertising databases. Whether it is an oil change at a national chain or a repair at a local dealership, your information is being collected. This will eventually result in related advertisements at your home and direct marketing toward your preference in vehicles. An average visit makes the following information available.

- ✓ Full name, home address, and home telephone number
- ✓ Cellular telephone number for pickup notification
- ✓ Make, model, year, mileage, registration, VIN, and maintenance history of vehicle
- ✓ Services provided and services declined
- ✓ Estimated warranty expiration

This is the type of information that companies such as TowerData and Epsilon use to build custom profiles on you. This is why you receive mailings from auto dealers and warranty providers at specific times. Staying out of this system is difficult, but not impossible.

Your best option is to locate a trusted individual to service your vehicle either in a small shop or home. It is more affordable, service is usually superior, and you leave no trace. If you must visit a repair shop or dealer, never provide your real name and address. Use the information available about you in the first tier. Payment can be made with your secondary credit card in your alternate name. Is this overkill? Maybe. Use your best judgment.

Smart Phone Applications

If you have a smart phone, you probably have numerous “apps” on your phone that do amazing things. Every time that you install one of these applications, you are asked to agree to the amount of data that the application will have access to on your device. Most people agree to these terms without reading the details. This can expose you to great risk of divulging your personal information. There are many examples of these sneaky applications on the internet, but I will only document one here.

True Caller is an app for Android and iPhone telephones. It is marketed as an application to provide phone number search and spam blocking features. You can set a list of people that you do not want to communicate with, and the software will forward these callers to voice mail without bothering you. Further, it will display the caller ID of many callers even if they are not in your contact list. Their website claims that the service will identify over 2 billion incoming telephone numbers. This includes both landlines and cellular numbers. This level of identification is impressive, which made me investigate how they collect cellular number information.

True Caller collects contact information from the telephones that it is installed on. When you install the application, it reports your entire contact list to a server. These entries are then added to a master database. If you had a friend’s private number stored in your telephone as “Brad O’Neal”, the number and name assigned to it are now in the database. If I install this application, and he calls

me, the application will tell me that his name is “Brad O’Neal” without me already having his information stored. It will further identify personal details such as employer and a photograph if available from a public source such as LinkedIn. This is referred to as crowd sourcing. The hundreds of thousands of users that installed this application gave possession of their contacts list to True Caller to do whatever they want. How did they legally do this? The permissions required from the application should give the answer.

Every application on the Google Play store must document the permissions required from the device to function. These are the areas of information that the application can have access to. When you install the application, you will be asked to approve or reject these permissions. If you reject them, the software will not install. The following permissions were extracted directly from True Caller’s Google website. This application is allowed to:

- ✓ Read your contacts
- ✓ Add or remove accounts
- ✓ Modify your contacts
- ✓ Know your approximate location (network-based)
- ✓ Read your text messages (SMS or MMS)
- ✓ Directly call phone numbers
- ✓ Reroute outgoing calls
- ✓ Modify or delete the contents of your USB storage
- ✓ Read the contents of your USB storage
- ✓ View Wi-Fi connections

- ✓ Read phone status and identity

Some of the items on this list explain how this company can legally copy your contact list and add it to their database of numbers and names. You give them permission to do this when you agree to these terms. Now everyone in your contact list has lost the privacy of their cellular and landline numbers. Also, any of your friends that installed this application have now shared your contact information that is stored in their telephone. If this were not bad enough, the service will also let anyone type in a telephone number and display the caller ID information stored on the database. It eliminates the need for you to call someone for them to identify your number.

I do not mean to pick on True Caller. There are thousands of applications that require you to grant similar permissions. I recommend that you read the permissions that you are granting to every application that you install. If something looks wrong, do not install the application. In my experience, the applications that offer any free service to interact with your telephone calls, text messaging, caller ID, or contact list are extracting all information from your telephone. It is not worth jeopardizing the privacy of you or your friends and family.

If you navigate to truecaller.com, you can search the database of collected caller ID information. If you were to type in the cellular number assigned to my previously issued government phone, you would receive a result of “Mike Bazzel”. This tells me that someone in my former government circle installed this app on their device.

Monitoring

Now that your information is out of public view, you must continually monitor the entire internet for any new information that may surface. Recent studies have identified over 55 billion web pages in existence. The hard way to do this would be to scour Google every day looking for anything new identifying your information. Do not worry, this monitoring can be automated.

Google Alerts (google.com/alerts)

Google is a very powerful search engine. It can identify areas where your personal information, such as name and home address, are on display in a public website. Manually searching every week or month is a burden. Google Alerts can automate this search and send you an email when any new results appear. This free service will basically notify you when your information has appeared on a public site.

- ✓ Log into your new personal Gmail account. If you do not have a Gmail account, navigate to gmail.com and create a new free account.

- ✓ Determine the exact searches of your personal information that would return appropriate results. This will vary depending on how common your name is. If your name is unique, such as Jeremiah Dressler, and you live at 4054 Brenner Street in Biloxi, MS, you should create the following alerts.

"Jeremiah Dressler"
"Jeremiah Dressler" "Brenner"
"4054 Brenner" "Biloxi"

- ✓ The quotes should be included in the alert. If you have a child named James, you should also add an alert for him such as "James Dressler" "Brenner".

- ✓ However, if you have a common name, you will need to add more data. If you do not specify the exact search that you want, you will receive too many false positives for pages that are not about you. If your name is Brian Johnson, and you live at 1212 Main in Denver, CO, you should create alerts that are specific to you. These should include interests, a workplace, or associations. The goal is to search for the perfect amount of data to identify your public personal leaks without receiving irrelevant data. You will need to manipulate these searches until you achieve only the results that are about you.

"Brian Johnson" "1212 Main" "Denver"
"Brian Johnson" "volleyball" (a specific interest)

"Brian Johnson" "Denver" "Johnson Ford" (workplace)
"Brian Johnson" "Denver" "Colorado AARP" (association)

- ✓ If your landline telephone number is 314-555-1234 and your cellular number is 713-555-9999, you should add the following alerts.

"314-555-1234"
"314" "555-1234"
"713-555-9999"
"713" "555-9999"

These specific search terms will attempt to locate information placed within websites that match the terms inside quotes. For example, if a person search site created a new profile in the name of Jeremiah Dressler, Google would pick up on this and let you know. If a reverse telephone directory listed the term "Jeremiah Dressler" and the street of "Brenner" in the same page, this service would alert you. The quotes mandate that a result is only returned when those words are next to each other on the page. The telephone number examples would identify a website with your number even if the area code was separated from the rest of the number.

- ✓ Navigate to google.com/alerts. Supply the first alert that you want to create. The result type should be "Everything", frequency should be "As-it-happens", results should be "All results", and the delivery should be to your Gmail address. As you create the alert, you will see the current search results in the right column. Click "Create Alert" when complete and continue to add alerts.

- ✓ Click on the "Manage your alerts" button and review your alert settings. Here you can modify or delete an alert that you have created.

With a properly configured set of Google Alerts, you can be notified in real time as Google finds information about you and your family. You are not limited to these examples. I have alerts in place for my website and book. If any website links to my website, or someone is discussing my other book, I can be notified

and provided a link to the source. I also have alerts for “Michael Bazzell” and “Mike Bazzell” in case someone uses my shortened name.

Google Analytics (google.com/analytics)

This book has discussed how websites track you and collect information about your internet searches and history. You can use this same technology to track people that are looking for information about you. You can know when someone searches for you on Google, where they are located, and what they were researching in order to find you. This may sound expensive and difficult. The easiest way to apply this tracking technique is to create a free website and add Google Analytics.

- ✓ Navigate to sites.google.com and log in with your Gmail account information. Click the red “Create” button to start a new project.

- ✓ Provide the name of your site. This should be your real name. Contrary to the rest of this book, you want people to find this website. For the site location, supply your real name without spaces. If that name is taken, add generic information to the end of the name. If your name is Chris Johnson, “ChrisJohnson” will probably already be in use. Try “ChrisJohnsonHomeAddress”. This will make more sense in a moment. Select the “Create” button to generate a new generic website.

- ✓ Click the small icon that looks like a pencil. This will allow you to edit your new website. For this site’s purpose, change the title to “YOUR NAME’s Home Address”. Obviously, enter your real name. In the content box below it, type any names that you think people would search to find you. Since I have a fairly unique name, I have included different spellings of my last name with the full and shortened versions of my first name. I also included “telephone number” and “phone number”. Notice that I did not actually place my number here, only a reference to it. Click “Save” when you are finished. Now, when someone conducts a Google search for “Mike Bazzell home address” or “Michael Bazel phone number”, this new site will be in the results. If you have a common name, you may want

to consider adding any term that is very public about you that would help with this bait, such as the name of your spouse or the high school you attended. It is important that you not include any information that would identify your home or children. You only want to make it easy for someone to find this page through a search.

- ✓ Navigate to google.com/analytics. Select "Create an account" and click the "Admin" tab in the upper right portion of the screen. This will present a page with a button labeled "+ New Account". Click this button. In the "Account Name" field, type your real name. In the "Website URL" fields, select http:// and then type the location of your new website. This will be the name you used earlier without spaces. In the example, I used "ChrisJohnsonHomeAddress". If this was your example, your entire Google website address would be sites.google.com/site/ChrisJohnsonHomeAddress. If you have trouble with this, go back to the website that you created. When you can see the website, look at the address bar. It will display the exact URL of your site. Agree to the terms and click "create account".

- ✓ On the next page, ignore everything and click "save". At the top of this page will be your new Google Tracking ID. It will look like UA-33333333-1. Select this entire ID and copy it.

- ✓ Return to your new Google website. Select the "more" button and click "Manage Site". In the "Statistics" portion of the page, check the box labeled "Enable Google Analytics for this site". Paste in the number you previously copied. Click the red "Save" button. It may take up to 24 hours for Google to add the analytics to your site.

- ✓ Navigate to google.com/webmasters/tools/submit-url. Enter the entire website address of your new site. In the previous example, it would be sites.google.com/site/ChrisJohnsonHomeAddress. Click "Submit Request". This notifies Google and requests that they scan your website for keywords to be added to their search index. This will make the website appear in a search result when someone is trying to locate you. It may also take up to 24 hours to be activated.

In summary, this process created a free website with limited information about you in plain view. This will only be your name and possibly some other content that is not private to you. Since you added Google Analytics, you can track the visitors to this site and learn information about them. This will often identify why a person is trying to find you. You should now visit your analytics site and see what you find. There is an abundance of data available about the visitors to your website. Most likely, you will have very few visitors, if any at all. When you do receive visits, the Google Analytics portal will let you browse the data collected from the visit.

Analytics Reports

Now that you have Google Analytics installed and monitoring your website, you are ready to view reports about visitors.

- ✓ Navigate to google.com/analytics. Sign in to your Google account and select the name of your website. This will present an overview page of traffic to your site. If you see that there were no visitors, then you know that no one was at your site for the past 30 days. There is nothing else to see here. However, if you have visits, continue to the next step.

- ✓ In the left menu, click “Demographics” in the “Audience” section. Click “Location” and view the map to your right. This will identify the locations of people visiting your website. The dark green states have had the most visits and the white states have had no visits. Clicking on a state will open the state view and identify which cities have visited your site. This will never disclose the name of the person searching for you, but knowing the city and state the person is in could be helpful. The data also identifies the number of visits and the average time spent looking at the site.

- ✓ In the left menu, click “Traffic Sources” and then “Overview”. This will present a summary of how people found your website. This will probably all be through search traffic. Scroll to the bottom of the page and view the data in the lower right portion. These are the exact searches that were typed into Google.

This will be an important area to monitor on your website. If someone does visit your page, you can identify the terms that were typed to find you. A search of your name may not concern you. However, a search of “Mike Bazzell home address” from a location of a past stalker should raise your interest. The following true story may shed light on why this process is important.

In 2010, I was asked to assist with creating a Google Analytics site for a client receiving serious death threats. He suspected it was the family of a federal prisoner that he had testified against. A few months after the analytics were active, someone from Minneapolis, MN conducted a search on Google for my client’s name and the term “address”. A quick search of the suspect on the Federal Bureau of Prisons website verified that the suspect had just been released from federal custody. He had been housed in Minneapolis, MN. This was an early notification that this suspect had not forgot about my client.

If you have been the victim of harassment or stalking, you should execute your own bait website. I also believe that targeted law enforcement personnel should consider using analytics now instead of waiting until a problem arises.

Chapter Fifteen

Major Life Events

This chapter will cover some, though certainly not all, major life events. If you encounter a life event or situation that is not explicitly covered by this situation I hope that the examples here will guide your thinking process.

Purchasing a Home

If you are planning on purchasing a home, this is a huge opportunity to make it practically impossible to be located from an internet search. Chapter Eleven explains how your publicly visible property tax record will inform dozens of data mining websites of your home address. This data will be acquired by many websites and you would need to remove the data from each site. Instead, consider starting life in your new home without attaching your name to the residence.

This method is only for those that are truly committed to being invisible from the public. The general idea of this process is credited to J.J. Luna, the author of the book ***How to be Invisible***. The basic premise of this specific method is the following:

- ✓ Purchase an official LLC from a registered agent in New Mexico. These are never publicly associated with your real name, but you own the business. These are very affordable.

- ✓ Purchase your new home using the LLC as the owner. The LLC can also purchase vehicles and other property.

- ✓ Never associate your name with the house you live in. Personal mail should be delivered to a PO Box. Utilities should be in the name of the LLC.

If you are at all intrigued by these possibilities, Luna's book is a good primer. The methods are completely legal. Mr. Luna provides recommended services in New Mexico that will make the process easy. If you are in any way targeted by someone, such as police officers or victims of harassment, this will guarantee that you will have a home private from the internet. For more information, visit jjluna.com and select the New Mexico LLCs tab. While I will disclose my experiences with New Mexico LLC's in this chapter, I insist that you always consult with a real estate attorney before you commit to your invisible home purchase. It will be money well spent. I have worked with many people that chose the path of an invisible LLC as the owner of their home. I have selected two common scenarios to present to you. Both may help you determine if this method is appropriate for your situation.

"John" purchased his New Mexico LLC through Luna's service. He dealt with "Rosie", the registered agent for this service. He provided a generic 33 Mail email address during the purchase that forwards to his primary email account. This meets the requirement for notification by the registered agent that is included with the purchase. If a subpoena were delivered to the New Mexico agent, she could forward it via email. John would not necessarily need to give his real name to the agent. He paid less than $400 which includes three years of registered agent service. He used a Blur masked credit card. He received his paperwork and confirmed the LLC through New Mexico's business lookup website. He is now the owner of an invisible LLC.

John chose to register this business with the Internal Revenue Service (IRS). He associated the LLC with his own Social Security Number (SSN). Some privacy advocates do not endorse this step. I believe that it is a smart move. It will definitely create a connection between his invisible LLC and real identity. However, this is only visible to the IRS, and is not publicly visible. I promote this for several reasons.

- ✓ The IRS will assign an Employer Identification Number (EIN). This will be required in order to open a business checking account, if

desired.

- ✓ The IRS will have a record of this business name, creation date, and association with you. If anyone were to challenge the true owner of the property, this record could work in your favor.

- ✓ The LLC will never have any income, therefore there will be no taxes due.

- ✓ Legally registering this business with the IRS eliminates most appearances that you are trying to hide or launder money. This overt action may work in your favor if ever audited.

Creating the EIN number was conducted through the official IRS website and was immediate. He registered the business as a sole proprietor. The state of his full-time residence was not relevant. He will now include this EIN on his tax return yearly, but will claim no income. His accountant will fill in the proper information.

John now had the LLC in place and an EIN to use when appropriate. He identified the home he wanted to buy and had a real estate agent that he liked. He chose this agent after interviewing five candidates. At my recommendation, he asked the following question to each of the potential agents.

“How do I buy this home using my LLC and not providing my name?”

One agent stated that this was impossible, and she was immediately eliminated. Two agents stated that it should be no problem and that they would work it out at the closing. These two were also dismissed. One agent declared that he really did not know, and withdrew interest. The final candidate stated that it was absolutely possible, but there would be many requirements that John would need to work with. He further stated that a cash purchase would be the easiest way, that a real estate attorney should look over everything before closing, and John should not be present at the closing. I liked this agent.

John paid cash in the form of a bank money order for this modest home. He paid a real estate attorney $500 to verify that everything was in order. John gave limited power of attorney to the real estate attorney, and this person signed the appropriate paperwork at the closing on behalf of the LLC. Everything was smooth, and it was a bargain at $500. John's name was never disclosed anywhere on any paperwork. Only the LLC was identified as the owner. The LLC is not publicly associated with John. There is no trail for anyone to follow.

I respect that John is a rarity that can pay cash for a home. Therefore, I also want to tell you about "Jane" and her experience. Jane identified the home that she wanted but only had 10% of the price as a down payment. In this scenario, she has no choice but to disclose her true identity to the bank issuing the loan. She had already obtained the invisible LLC that would be used as the actual owner of the property. She did not register this LLC with the IRS, which is completely legal. She would not be using it for any income, she was the sole proprietor, and the LLC would never have any employees. Since she was obtaining a loan in her true name, there was little need for additional protection from the IRS.

When Jane met with a loan specialist, she quickly declared that this would not be a traditional loan request. She stated that she would be titling the home in the name of an LLC and that her name would not be associated with the property. She was promptly informed that this would be impossible. As I had instructed her, she politely walked out of the meeting. I had a backup plan.

I contacted five major home loan providers and scheduled a call with each for the purpose of negotiating a loan rate. I scheduled this call for the same time for each provider. I stated that the subject of the loan would also be on the call and that I was acting on her behalf. I disclosed her true identity and SSN in order for a preliminary credit check to be performed before the call. I did not disclose to any of the providers that other companies would be involved.

This gave the loan specialists an opportunity to discover that Jane was a great candidate for a loan with good credit. I provided her desired house price range, amount available for a down payment, and time frame for purchase. I never disclosed her current location, but this would not have been much of a compromise. Her name was already publicly attached to her current residence through numerous websites.

I arranged a telephone conference line that I could use for one hour. The cost was less than $15. On the date and time of the scheduled call, I contacted each loan specialist and placed them on a brief hold while I “patched in Jane”. While I brought Jane into the call, I also connected all five providers at the same time. I stated that Jane would like to negotiate the best rate possible, and would only be accepting offers during this live call. Before I opened the floor to the frustrated providers, I explained that the loan must be in the name of her LLC. I further clarified that she would be responsible for the loan and understood that she would need to co-sign at the least. I was adamant that her name would never be disclosed during the closing process. Only the LLC would be listed as the owner on the deed for the home. I acknowledged that she was the sole proprietor of the LLC and then confirmed the loan would be the responsibility solely of her as an individual.

One loan company ended the call right away. One sat quietly and just absorbed the entire situation. The remaining three presented their best offers. Two of them lowered the interest rate and began a bidding war to compete for the loan. The winner offered a rate that I was unable to find advertised anywhere. Jane was thrilled.

Many people enter a bank and plead for a home loan. I look at it differently. The bank should be begging you. You will be paying them tens of thousands of dollars in interest. I believe THEY are the employee and YOU are in charge of the process.

Obviously, there are flaws with this method. Associating Jane with the loan can be dangerous. If her details leak out, she would be compromised. With her situation, there was not much else as an option. I was not worried about the bank releasing any information. They keep financial details fairly secure. The title company that conducts the closing process is the only concern. As long as they do not know who Jane is, it should stay out of public record. I insisted that she hire a real estate attorney to review everything and sign at the closing as her limited power of attorney. She insisted on attending the closing. She attended as the attorney’s intern and signed nothing. Jane now believes that she is a ninja and I think that I may have created a monster.

The main lesson here is that a truly invisible home is possible. You will likely be

met with resistance along the way. Do not let that deter you. When someone says that you cannot do this, find a different professional. Always remember that these people work for you, not the other way around.

Over the past few years, I have spoken with several readers that were not ready to make the jump into invisible LLC’s. I completely understand and agree that the idea of placing your largest asset into the name of an LLC that is not registered to you can be overwhelming. Additionally, this can be difficult when there is a lien on the home. The following option does not provide the same level of privacy as an invisible LLC. However, it will help shield your real name from public records.

Many people choose to make the owner of their home a revocable living trust. This is usually not associated with privacy protection. A living trust is a legal entity that many people use for the distribution of wealth when they die. A will can be beneficial, but it is subject to probate. This means that your wishes detailed in your will are not executed until approved by the probate court. This can take years. A living trust avoids the probate process altogether.

To create a revocable living trust, you (the grantor) transfers ownership of some or all of your property to the trust. Because you make yourself the “trustee," you don't give up any control over the property you put in the trust. If you and your spouse create a trust together, you will be co-trustees.

In the trust document, you name the people or institutions you want to inherit trust property after your death. You can change those choices at any time if you wish. You can also revoke the trust completely. When you die, the person you named in the trust document to take over, called the successor trustee, transfers ownership of trust property to the people you want to get it. In most cases, the successor trustee can handle the whole thing in a few weeks with some simple paperwork.

Essentially, you can create your own revocable living trust by completing a form. There are numerous versions online or you could create one using a word processor. This printed trust identifies the name of the trust and the assets that are owned by the trust. This document should be notarized and witnessed by at least two trusted subjects.

Trusts are extremely common with home owners. Often, a retired person will transfer any property, including a home, into a trust as part of estate planning. If you are buying a new home, you should consider taking this step now instead of later. This will keep your name out of many public databases.

Before you purchase the home, you should have your revocable trust complete and active. You do not need to generate an EIN number with the IRS. You will need to give your trust a name. Most people choose something obvious such as “The Michael Bazzell Living Trust” or “The Bazzell Family Living Trust”. Using personally identifiable information is not mandatory or recommended. Instead, consider something generic such as “The Private Life Living Trust” or “The Partners Living Trust”. These names do not associate you with the trust.

Once you have created the trust, you need to add your assets. You cannot add cash, but you can add property, real estate, collectibles, and financial accounts. Many people that I consult have all of their wealth in the name of their living trust. Financial accounts will still be associated with your real name and social security number. This is important to prove ownership.

When you close on your new home, consider allowing your real estate agent to sign the paperwork on your behalf. Make sure he or she understands your desire to place the title for the home in the name of your living trust, and not in your name. Financial institutions are familiar with this process and should allow this during your loan process. Obviously, any loan will still be in your name.

If you already own your home, and moving is out of the question, you can transfer your home into the trust. This will require filing a quitclaim deed at your county assessor’s office. This is a very standard practice that should not raise any suspicion. Your home address will still be associated with your real name on several websites, but new information that is collected will replace your name with the name of your trust. This will eliminate a lot of new entries associating you to your home address.

I want to stress the importance of consulting with a lawyer when creating your living trust. I also recommend reading any books by Nolo on the living trust creation process. The minor expense that you spend to make all of the documentation correct will pay off tenfold when you die and your heirs are left

with your assets. Additionally, having the correct and accurate paperwork will aid in a smooth process when placing a home in the name of the trust.

Renting a Home

Renting can have advantages and disadvantages in regard to protecting your privacy. Some places include all utilities which is a huge privacy layer. If the utilities are already in the landlord's name, you never need to provide your information to the utility companies. Unfortunately, most rental agreements will require your full details for a background check. You may also be asked to obtain an occupancy permit. The following suggestions will get you through these roadblocks.

Avoid large complexes. Apartments and condominiums that are maintained by larger businesses have strict rules on processing applicants. You will need to pay a fee to have them conduct a complete history, criminal, and financial background check on your real information. If you pass, you will then be required to use your details for all utilities and permits. Look for homes and apartments owned by individuals. They will be more willing to accommodate a good renter.

I recommend applying Luna's method of obtaining an invisible LLC for renting. Your LLC can rent the place and pay the bills. Many renters welcome this arrangement. Receiving money every month from a business is more reliable than from an individual. People that I have consulted in similar situations have had the best results with the following techniques.

Find an apartment or home that is a prospect for rental. Notify the owner right away that the company you work for is relocating you and will be paying the rent. Provide the name of the LLC and your post office box address. Offer to pay a month in advance and have a check from the LLC ready for the deposit. Be polite and look professional.

Another option is to notify the owner that you have been the victim of stalking or harassment and you are looking for a new safe place to stay. Explain your concern about making your information public. This tends to work best for

females or families with children. Overall, be courteous and respectful. Offer to pay an additional month of rent in advance in order to demonstrate your ability to make the payments.

LLC Bank Accounts

Regardless of your method of using invisible New Mexico LLC's, you will likely need a business checking account to take full advantage of this layer of privacy. While some privacy advocates discourage any use of business banking, I embrace the necessity. Using cash to order new utilities, pay your monthly mortgage, or hire labor services is not always an option. Today, it also makes you look guilty of something. I hate this, but I must accept the world we live in. Therefore, I believe it is important to possess a business checking account if you have an invisible LLC.

This is not an easy task. I have been denied more business accounts at banks than I have been successful. As with everything else, diligence will pay off in the end. Hopefully, my research will help you and your journey for anonymity.

I contacted numerous banks and credit unions with the intent of opening a business checking account in the name of an invisible LLC. The odd requirement was that I would not disclose the owner of the LLC or the SSN of the client. New federal laws post 9/11 have made this very difficult. Many bankers believe that obtaining the SSN of the account holder is absolutely required. While the bank's policy may require this, the law does not. They are only required to obtain either the SSN of the individual or EIN of the business. Convincing the bank of this is often impossible.

Most of the large chain banks that I visited absolutely insisted that the person that opens the business account must provide their true name, home address, SSN, DOB, and copies of two forms of government identification. I found local credit unions to be a bit more accommodating, but they still wanted ID and a SSN. In order to skip directly to the two initial successes, here are the best results.

During one of my training sessions, I met a privacy enthusiast that had just

obtained his invisible LLC. He was ready to open a bank account and asked if I was interested in an after-class road trip. I took the bait and drove with him and his brother to an Associated Bank in his town. I developed my strategy on the drive there. I went in and sat down with a banker. My new friend was nervous and allowed me to do the talking. Before you think I am crazy for this, know that he was employed by a federal agency that is in the same circles as those in my background. This brought a little comfort.

He had targeted this bank because his initial telephone calls led him to believe that they would not require a SSN. I stated that I wanted to open a business checking account. I provided the New Mexico LLC certificate, the IRS letter including EIN, $2,500 initial cash from the owner, and a contract identifying his brother as the “organizer” of the LLC. This was also referenced in the articles of organization that I provided. I completed some paperwork, had his brother sign the documents and allowed the banker to make copies of the documentation.

Eventually, the banker asked for the brother’s SSN. I interrupted and stated that the business would only like the account associated with the EIN as provided by the IRS. Since the brother was not an owner of the business, it would be inappropriate for the brother to disclose his own SSN. To my surprise, the banker was not bothered by this. The brother had to provide photo government identification. He was prepared with his passport that did not include a SSN or home address.

It should be noted that the brother had a different last name than my friend. This was a nice layer of privacy. Only the bank knows the owner of the LLC. These bank records should stay private. They will definitely not be visible on the internet. My friend left the bank with a new business checking account, temporary checks, and official checks on the way. He only provided a PO Box as the address of the business. He disclosed that it was a home based business and nothing else was required. The bank met its obligation by obtaining the EIN assigned by the IRS. The IRS should be content since we have now associated the banking account to the true owner in their eyes.

I believe that financial institutions in every area will be unique. Large chain bank branches in one town may be more willing to accommodate than identical banks in other cities. Your experience will likely be unique from anything that I can

print. However, below is a table that displays financial institutions and my results when attempting to open business checking accounts.

Institution	EIN Required?	SSN Required?	Balance to avoid fees:
Associated Bank	Yes	No	$2,500
Bank of America	Yes	No	$3,000
Chase Bank	Yes	No	$1,500
Local Credit Union 1	Yes	Yes	$1,000
Local Credit Union 2	Yes	Yes	$1,500
Local Credit Union 3	Yes	No	$1,500
Local Credit Union 4	Yes	No	$2,500
US Bank	Yes	Yes	$1,500

Obviously, this list includes an extreme minority of available institutions. I only wanted to verify that this concept was plausible. I discovered that larger financial institutions seem to be the strictest. US Bank absolutely refused to entertain the thought of not collecting someone's SSN. I found this to be the case at three locations. Because the option was on the application, it was mandatory. Bank of America's application also included a mandatory SSN field. However, I was allowed to open an account with only an EIN. While I could not do this over the internet, a visit to their physical branch worked fine. On one occasion, I simply stated "I don't have a SSN, I only have this letter from the IRS with my EIN on it.". Exactly 50% of the credit unions that I contacted allowed business accounts with only an EIN. Chase allowed me to use only an EIN, but demanded two forms of identification and all members of the business to be present. I was allowed to nominate an organizing member and she only had to show a passport and utility bill (neither display a SSN).

This resistance is likely due to policies and not interpretation of law. I encourage you to start with the smaller banks and credit unions in your area. Explain your situation and dress nice. Speak clearly and confidently. I do not encourage you to open a business account anywhere that you already have personal accounts in place.

Anonymous Utilities

Whether you live in a house owned by an invisible LLC, home titled to a living trust, or apartment in the name of your landlord, you must take care in establishing your utilities. A previous chapter already mentioned acquiring anonymous internet service. Obtaining electricity, gas, sewer, trash, and water can bring complications.

If your home is in the name of an LLC, I encourage you to continue this appearance and assign your utilities to the LLC. When you contact each company, tell them that the home is owned by a business and that you want to set up the new account. Identify yourself as a representative of the business and declare that you will not be living at the house. If pressured, tell them that employees temporarily assigned to the area will stay here as needed. Offer to pay a deposit and sign up for automatic withdrawals from your business checking account. If they push for a SSN, offer the EIN assigned to the LLC. This should suffice.

If your property is in a living trust, you may consider an invisible LLC solely for the utilities. You can also try the prior instruction and ask the bills to be assigned to the trust. If pressured, tell them that you are calling on behalf of your grandmother and that the house is in the name of the trust. State that she insists that the bills match the deed for the home. Many people that are not familiar with living trusts associate them with elderly people near death.

If you are renting, ask your landlord if you can keep the utilities in his or her name. Offer to prepay and have a sob story ready. If he or she refuses, you could consider either the LLC or living trust methods. Most importantly, never place the utilities of your invisible home in your own name or the name of anyone close to you. This will immediately compromise your location.

I recently spoke to a potential client that had tried everything she could think of to place her utilities in an alias name. She had been denied during every attempt. While she had practically given up, I had one last idea that could work for her. With some brief coaching, she provided the following details to a well know power company when asked for her SSN and DOB.

“I do not have a SSN. I am not a U.S. citizen; I am just here attending school full time. I have a credit card for a deposit if that helps. Do you want my Personal

Identification Number?”

To be very clear, this is obviously a lie. However, I could find no state or federal laws that declare lying to a private company about utility service a criminal act. As long as your intentions are good and you pay your bills, there is no fraud in my opinion. She provided a random “Personal Identification Number” to the operator, which does not exist. Her credit card was charged a $100 deposit and a small convenience fee. I considered this a fair trade.

Vehicle Purchases

The preferred way to stay anonymous throughout a vehicle purchase is to pay cash to an individual. This is not always ideal depending on the type of vehicle that you want. I believe that vehicles should be the property of, and registered to, an invisible New Mexico LLC. At the very least, they should be attached to a revocable living trust. They should never be registered to your real name. This is based on years of monitoring criminal behavior and erroneous lawsuits. Consider the following true scenario.

Several years ago, I was interviewing a criminal that had brutally attacked the driver of a vehicle that unintentionally cut him off in traffic. The victim had a faster car than the attacker and sped away before anything bad could happen. Though the victim had gotten away and felt safe in his own home, the attacker showed up at his door. A fight ensued and the victim was left permanently disfigured. During the interview, I learned that the attacker had received the home address of the victim through his license plate registration. These queries are only available to law enforcement and a handful of companies, so I was intrigued by how he was able to do this. He gave the following account.

After the road rage incident, the attacker was at home and furious about the event. He wanted revenge. He had written down the license plate of the victim and wanted to know where he lived. He turned on his police scanner and monitored the channel of his local police. He then called that police department and reported a drunk driver all over the road at a nearby location. He provided the actual license registration of the victim. He then listened to the police scanner as the dispatcher advised patrol units of the reported reckless driver. At the end of the dispatch, the patrol units were told the name and address of the

victim according to the registration. The attacker had now heard what he needed to confront and beat the victim.

Having your vehicle registered to either an LLC or trust would save you from this type of attack. The offender would only know the name of your LLC or trust and a PO Box that receives mail. However, a trust will provide you no protection from erroneous lawsuits. Having your vehicle owned and registered to an invisible LLC will provide you an additional layer of protection. Nothing will make you 100% lawsuit-proof, but every layer can help. Consider the following.

Within 30 days of purchasing a new vehicle, data brokers know every detail about you, the vehicle, and how it was financed. If you have any doubt about this, request your personal report from LexisNexis and others as instructed in the previous chapters. You should see the details of every vehicle at your residence and information about the licensed drivers. The report identifies the full name and home address of the owner. The vehicle information includes the year, make, model, VIN, weight, wheel base, base price, size of the vehicle, vehicle's registration, title number, and lien information. If you are still not convinced that this is an invasion of your privacy, consider the following.

Accident attorneys, sometimes referred to as "ambulance chasers", make a lucrative living from suing people involved in traffic crashes. Some of their clients come to them seeking damages, but an overwhelming number of lawsuits are generated by the attorney. Lawyers can go to a police department and request a copy of every traffic crash report for an entire month. These redacted reports include the names of the vehicle owners and the insurance companies providing insurance on the vehicles. The reports are modified to mask the name and home address of the subjects involved. This request must be allowed because the attorney filed a Freedom of Information request. The police department must comply. I have personally witnessed teams of lawyers sit in the police lobby and look through the reports for traffic crashes involving expensive vehicles owned by the driver at fault. They then conduct a quick internet search on the vehicle owners and respond to the victim's home to encourage a lawsuit.

If you are involved in a traffic crash, you cannot keep the vehicle owner's name from appearing on a public report. You also cannot hide the details about your vehicle. You can keep your name from the public version by purchasing the

vehicle with your new LLC. When you buy a new or used vehicle, notify the sales person that you will be purchasing the vehicle on behalf of a business and that the registration and title should identify the business as the owner. This technique is explained in J.J. Luna's book, ***How To Be Invisible***. With this method in place, the nosy lawyer will only know that your LLC owns the vehicle, and will not have a name to associate with the vehicle. If a lawsuit is filed, the attorney can make a new request for the complete report, which will identify you. However, the mass search will mask your details. Please note that this does not hide your details from the other party involved if they request a report. It also does not hide your details from the police department investigating the incident.

Senseless acts like these are reasons why I recommend purchasing and registering any vehicle as an entity and not an individual. The idea of an invisible LLC discussed earlier may not have been ideal for you when buying a home. However, you may be more comfortable with this tactic during a vehicle purchase. For many people, registering their vehicle to an LLC or trust is the gateway toward complete anonymity with all future purchases. There are several possibilities for this, and I will outline various scenarios here to give you an idea of the best formula for your needs. Each method identifies the type of purchase, payment used, and method of identity protection.

- ✓ Individual-Cash (LLC): If you possess an invisible LLC from New Mexico, this is the ideal way to go. Give the individual cash and obtain a valid title. Take the title and your LLC paperwork to a local vehicle title shop and have them complete the proper process for registering the vehicle. This type of business will be much more accommodating than the Department of Motor Vehicles (DMV).

- ✓ Individual-Cash (Trust): After you have created your revocable living trust, give the individual cash and obtain a valid title. Take the title and your trust paperwork to a local vehicle title shop and have them complete the proper process for registering the vehicle.

- ✓ Dealer-Cash (LLC): Staying anonymous at a dealership is not difficult, but it will take some diligence. Having the resources to purchase a vehicle without a loan will aid in this process. When you

first meet the sales person, advise them right away that you are shopping for your boss and that the company (LLC) will be purchasing the vehicle. The dealership will facilitate the registration process and you should demand that all information is in the name of the LLC. While you cannot use a PO Box on your driver's license, most states allow the use on vehicle registration.

- ✓ Dealer-Cash (Trust): When you first meet the sales person, advise them right away that you are purchasing the vehicle in the name of your Grandma's trust. They will not know if this is true. The dealership will facilitate the registration process and you should demand that all information is in the name of the trust. Again, provide your valid PO Box and never give them your real address.

- ✓ Dealer-Loan (LLC): A dealer will not give you a loan in the name of an LLC or trust. This does not mean you cannot register the vehicle in the name of either. Complete the loan paperwork and demand that the vehicle is registered to your LLC. Inform the sales person that you will not complete the sale until you see proof that this is set up accordingly. I advise avoiding the loan process if at all possible.

- ✓ Dealer-Loan (Trust): Similar to the previous option, complete the loan paperwork and demand that the vehicle is registered to your trust. Inform the sales person that you will not complete the sale until you see proof that this is set up accordingly.

I can speak from experience that providing your real address when you purchase a vehicle is a bad idea. I purchased a new vehicle in 2003 and provided all of my personal information. I did not know better at the time. In 2005, I began receiving numerous advertisements referencing my vehicle and offering me discounted services. In 2008, I began receiving third party warranty options since my standard warranty was about to expire. My name, address, and vehicle information was in the hands of dozens of companies.

When you buy from a dealer, you cannot stop this information from being sold. However, you can control the information that is attached to your profile. When paying cash, always provide the name of an LLC or trust, a PO Box address, and

nothing else. Have a check ready for the sale that is attached to an account for the LLC or trust. Be prepared to walk away when a sales person begins pushing you for more information. They will always stop you and do whatever it takes to make the sale.

Marriage

When you get married, a great deal of new information is generated about you. Though most individuals wish to proclaim their love of another to the world, this information is fraught with privacy concerns. Weddings are matters of public record and are often published in newspapers and on the internet. You should consider this before getting married. If you are a high-risk federal agent, you may be endangering your partner by publicly marrying him or her. Before getting married, you should consider a few things.

The first consideration is whether you really want to get married. Many couples live happy, successful lives without the legal bond of marriage. I am not anti-marriage and I understand the social and financial benefits of it. I encourage you to seriously consider the commitment of marriage and the privacy implications it carries. If you decide to get married, my advice is as follows.

Consider a strictly religious ceremony: For those who have deeply-held religious beliefs, marriage may be mandatory. If you fall into this category and you are getting married for strictly religious reasons, it may make sense for you to have a religious ceremony only and forgo the legal formalities. Though you will not enjoy the financial benefits of marriage, you will be wed in the eyes of your faith and your privacy will remain intact. However, this will not convey many of the financial and legal benefits of being legally married.

Elope: I am a strong proponent of very private marriage ceremonies as far as the official proceedings go. By eloping with certain criteria in mind, you can avoid your legal wedding being publicized on the internet. I understand that many people dream of a large wedding surrounded by family and friends, and I do not ask you to deny yourself that privilege. If you wish to have a formal ceremony, you should. However, I encourage you to have a very small ceremony ahead of time. Ideally, it should consist of you, your betrothed, an officiant, and the smallest legally allowable number of witnesses. This private proceeding is the

one that will be officially documented and legally join the two of you.

When choosing a location to which to elope, there are two major factors to consider. First, it should be a city or township that does not digitize its records. There are still a few holdout towns that do not have digital, searchable public records. This is changing and may not always be the case. I believe that if you look diligently, you should be able to find such a place. Impoverished, rural towns in the deep south and the American west should be good candidates. The next major criteria to look for is a town that has no ties to either individual in the ceremony. The state in which you choose to get officially wed should not be a former residence, place of work, or place of birth of either party or any of their close relatives. It should also be a state to which neither party frequently travels for leisure purposes. This will significantly reduce the chances of a determined adversary locating the record of your marriage.

It should be noted that this may not be considered a perfect solution. Though the town in which you chose to get married may not currently digitize records, this may change at some point in the future. As computers and digital storage become cheaper and more readily available, an increasing number of municipalities are digitizing their records. You should not be surprised if you find that your records have been added to a state, county, or town database that is publicly available online. Even if the town in which you get married does digitize its records, you still have some protection. An adversary would have to know the state and town to search to find your record. If you choose randomly and do not leave a digital trail, your matrimony should remain somewhat private.

Do not advertise: Do not announce your engagement or ceremony in the local newspaper. This is a custom in some parts of the U.S., and is a major privacy compromise. Once it is on the internet it will be nearly impossible to totally remove. Additionally, it may also contain a photograph of you and your fiancé. Avoiding this may be very important for your level of privacy. It is also becoming increasingly common to have a wedding website. Though these websites are claimed to be private and available only to those who have a direct link, I strongly advise against this practice. As everyone reading this should understand, nothing on the internet is truly private.

Maiden names: I recommend that both spouses keep their respective last names

rather than taking a single shared last name. This is another suggestion which many people will take issue, but it offers some serious privacy benefits. If both spouses in a marriage keep their given last names, the couple has twice as many names to use in the future should the need arise. If both spouses take a single name, there is now twice the likelihood that the name will be compromised.

Wedding photographers: Many wedding photographers have prolific websites and a social media presence. Often after shooting a wedding, a photographer will post photographs on his or her website for viewing by the attendees or for self-promotion. This is something that you should be keenly aware of when hiring a wedding photographer. The ownership and use of your likenesses should be addressed in the contract prior to engaging the photographer's services. Photography is already a crowded marketplace. If your first choice refuses to budge on this issue, a competitor almost certainly will indulge.

I recently worked with a pair of clients who, following their wedding, realized that dozens of very intimate photographs had been posted publicly on the photographer's website. At that point, there was little anyone could do to protect the likenesses of the newlyweds. Though the photographer was agreeable to taking the photographs down, the couple had lost control of their likenesses. They will never know if their photographs were downloaded, and if so, by whom. It is far easier to stop this before it happens than it is to take corrective action retroactively.

I know that this is starting to sound overly paranoid. Please take a step back and consider something. Imagine that you are thirty years in the past. You have just been married and possess an album of paper photo prints from the wedding. Would you consider making thousands of copies and giving them to complete strangers? Would you call up your enemies and offer the collection to them? Even if there was no cost associated, I assume you would not. When posting or allowing photos online, this is basically what you are doing. You are sharing your intimate moments with the world.

Wedding registries: Wedding registries require you to give up a lot of information. First, you must give up the names of both yourself and your co-registrant. You must provide an email address, telephone number, physical address, and other invasive information. Wedding registries are excellent vectors

for collecting marketing information that is then sold to other companies in the wedding industry. If you register for your wedding, I obviously recommend using services like 33 Mail, Blur, notsharingmy.info, and Google Voice to avoid giving out real information to every extent possible.

Unfortunately, wedding registries also require that you provide a physical address to which your gifts can be shipped. Obviously it would be a bad idea to use your home address. Rather, consider using a commercial mail receiving agency. Though the U.S. Post Office may not accept Fedex or UPS packages, CMRAs will. Alternatively, if you are not in any particular danger, you may consider using the address of a bridesmaid or best man (with her or his prior consent, of course), your office, or another address that does not tie your name to your home address.

As I mentioned in the discussion of anonymous purchases, it is ok to have items shipped to your house as long as they are not sent in your name. This is difficult with a wedding registry, but it is possible. One couple who eloped to Montana managed to do it. In what seemed like a spirit of good humor they informed every invitee that they were registered as “Bonnie Parker and Clyde Barrow!” The happy couple’s family and friends had no problem remembering the names of the infamous duo and took it as a joke.

Divorce

One major disadvantage of getting married is the potential for getting divorced. When you get divorced, you are again faced with a situation that can create a great deal of information about you. The silver lining to divorce is that it may be a golden opportunity to create some new privacy for yourself. As I have mentioned earlier, relocating your residence is required to achieve total privacy. In the aftermath of a divorce, it is common for both parties to move. If you move, I recommend finding a new home to rent or purchase anonymously as described earlier in this chapter.

If you are a female who changed your last name when you got married, divorce presents an almost brand new start. You can change your name easier than males can. Further, you can likely keep your married name in common usage. I worked with a female client during the writing of this book that had been divorced for

several months. She works in the criminal justice system in a major east coast city and deals with many convicted felons who know her first and last name. Due to her financial situation and employment by her state's government, being completely "invisible" was not an option for her. I found an excellent opportunity to protect her privacy when she mentioned that she wanted to change her name back to her maiden name.

I advised her to order as many business cards as possible before her name change back to her maiden name was official. I recommended that she keep using her married last name for official business, and set everything else up in her maiden name. This created a good degree of safety for her as none of the convicts with whom she interacted would know her real last name. It took some convincing because her married name was emotionally laden, but she eventually agreed and now enjoys much more safety and privacy.

Death

A death in the family can cause privacy concerns as well. The passing of a loved one can be a traumatic time, so I recommend dealing with this well in advance. The greatest compromises I have seen that are related to deaths are obituaries posted in newspapers and online. Obituaries can reveal a great deal of information about you including the names of your parents, siblings, spouse, and children. It will reveal your relationship to the deceased and your hometown.

To avoid this, you should plan ahead of time. You have several options. First, you may request that your family not provide any obituaries or other family announcements. This is the most extreme option and one that may be difficult for you or your family. Next you may ask that your family use your middle name, common name, or a nickname.

A client that I worked with several years ago knew his father would pass within a few weeks. The client was retired but faced some very severe threats due to his thirty-year career as a federal law enforcement agent. Revealing the names of his surviving mother, wife, children, and other family alongside his own was out of the question. After explaining this to his family they agreed to use a shortened version of his middle name which was Alexander. He was listed in the obituary as Alex. This provided some light protection against his entire name being found

in a simple online search while still allowing the client and his children to be recognized in the obituary.

If you are not facing such grave threats but still wish to protect your privacy, you still have the right to request such consideration from your family. Rather than saying you are in danger, you may wish to ask to be called something else in the obituary. You may state “it made him happy to call me that” or “that was my special thing with Dad”. I recommend discussing this with your family now rather than in the immediate aftermath of a loss. Though this may be a difficult discussion to have, it is important to have it now. Deaths happen unexpectedly. When they are anticipated, the emotion involved can still make it hard to have such a conversation that your family may view as silly or selfish.

There are many other major life events that were not mentioned here. Hopefully, this chapter can provide some insight that could be applied to anything else that you encounter. As with most of this book, the biggest lesson here is preparation. Having all of the pieces together before a major decision will have a great impact on the outcome.

Chapter Sixteen

Data Leakage Response

Bad things happen. I know people that 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 chapter will provide immediate actions that can be taken to minimize the damage after a mistake has caused a data leak. Your scenario will likely fall into one of the following categories.

- ✓ Your home address or telephone number is posted online.
- ✓ Your photo 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.

Home Information Leakage

The most common personal data that will find its way online will be your home address or telephone number. As discussed previously, this data is bought, sold, and shared by hundreds of companies. If your home is titled in your real name, this will eventually end up online. Previous chapters discussed the removal and monitoring options, but did not cover the next actions. Overall, a timely response is vital. The moment that a website possesses personal information about you, a

clock is ticking until other sources acquire the live information.

The first step is to identify any opt-out resources. As discussed previously, most data collection websites will have information about the process for data removal. If nothing can be found, attempt to identify any option to edit a listing. Many sites will allow you to update your information in order to correct their records. This is the ideal time to provide disinformation. Finally, direct contact with the company may be required. Consider the following example from a client in 2014.

Home Information Leakage Example

A friend reached out to me after he discovered his home address associated with his name on a new people search website. He had already completed the process of removing his information from dozens of websites, and this one did not have an opt-out policy. I first attempted contact via email, but received no response. I then located a fax number and submitted a written request. Again, no response. I finally took more drastic action.

I used an online email sending service and created a brief, yet firm demand to remove the posted information. I used the techniques discussed in Chapter Eight to identify possible email addresses of various employees of the target company. I then executed a scheduled email send option and sent one message to each employee per day until disabled. Within seven days, his information was removed. I never received an official response, but my point was made. Your mileage may vary.

Photo Leakage

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 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.

Photo Leakage Example

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 that 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, 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. Monitoring is vital.

Financial Information Leakage

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 of 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:

SSN: support.google.com/websearch/contact/government_number

Bank or credit account**:** support.google.com/websearch/contact/bank_number

Signature:
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 does not offer an automated removal request. Instead, you must complete an email support request that includes your name, email address, and URL of the exposed information. You must also choose “Content Removal Request” as the reason for contact. This form can be found at the following website.

support.discoverbing.com/eform.aspx?productKey=bingcontentremoval.

Financial Information Leakage Example

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 that he claimed my client had defaulted on. 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.

Locating Vulnerabilities

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 function such as Disconnect which is mentioned in Chapter Four. 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 account numbers and social security numbers. If you do not want to continually conduct the same searches, you could set up a Google Alert as instructed earlier.

Reputation Information Leakage

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. There are only a select few scenarios where you can force content offline.

Reputation Information Leakage Example

In 2015, I was contacted by a woman that 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) that 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 the 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 which each 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://support.microsoft.com/getsupport?oaspworkflow=start_1.0.0.0&wfname=capsub&productkey=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 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 short clip of the video. This clip looped and repeats while people are reading the comment. It appears as a brief, poor quality video. I re-submitted my request to Google and the link was removed nine days later. The rest of the results on the first page of her Google search were legitimate websites that she approved. My work was complete.

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.

Criminal Information Leakage

Many new websites have appeared that host mug shots and associated criminal information of anyone arrested in select states. This varies based on state law that allows 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 that hope to benefit from your removal request. Most of these will remove your mug shot for $500. The only purpose of these sites are financial.

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 mug shot appears on one of these sites, I have only found one potential solution. Your results will vary with this technique. The following example will explain the process that I took for a client.

Criminal Information Leakage Example

I was contacted by a subject that 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 mug shot appeared on one of these extortion sites. Within a week, it had been indexed by Google. A search of his name revealed the mug shot 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 mug shot 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 mug shot 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 fairly 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. 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. Further, most of these websites are owned by the same entity.

Summary

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 two websites, but neither 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. As of this writing, there are no photos of me online. While that could change, it will only be after I give it my best fight. My home address is not connected to my name within any database, public or private. I only use VOIP numbers and never my cellular number from my provider. I use encrypted messaging apps whenever possible. While it took years, I believe that I have achieved the level of invisibility appropriate for me.

Many books about privacy will tell you that it is all or nothing. Some will say that you should abandon your friends and live in the woods or that you should never use a cell phone or the internet. I believe neither. I think that you should educate yourself and understand how data collection works. Then, decide what layers of privacy are most important to you. Finally, strategize and execute your custom plan of attack. I believe that you can establish the balance most appropriate for you.

Conclusion

To keep up with the changes in various methods of personal information removal, read my blogs at **inteltechniques.com** and **computercrimeinfo.com** and visit the links sections. There is a good chance that as you read this, new content has been posted about the very topic you are researching. You can sign up for my free monthly newsletter on either site.

Hopefully, you have now eliminated all of the personal online information possible. You have changed your habits and no longer associate your real name with your home address. You have provided disinformation when appropriate and have a grasp on how companies extract and share all of your sensitive details. You should now conduct a post-assessment. You may choose to wait 30 days before completing this process. Many companies take some time to remove everything requested.

You should first re-visit Chapter One and repeat the techniques that were explained. This should give an immediate indication of your level of success. Next, visit the various people search websites in Chapter Two and conduct a manual search for your information. You will likely see great results with this category. After you have determined that your information is no longer present, I encourage you to continually monitor your personal details online.

The battle for privacy is never over. There will always be someone trying to obtain your personal information for profit. You may never be able to stop all of it. Staying on top of the information available to the public will create a strong layer of privacy. Many attempt to achieve privacy only when safety issues arise. It is often too late. You will never regret removing personal information, but you may have regrets if you do not. Nothing is more important than your safety and the safety of your family. We live in a chaotic and unpredictable world. Please consider reclaiming your privacy.

The amount of personal information collected about individuals will continue to escalate. This is a new form of currency for many businesses. I have never seen such an effort to individually target someone for the purpose of advertising. You do not have to accept this new standard. Use the techniques described to opt-out of this system.

I hope that this book will change the way that you interact with websites and businesses in the future. Every day, your privacy is jeopardized when you execute your normal routine. Whether through a website shopping experience or an in-person encounter with a sales person, there has never been a higher demand for your private details. Consider the lessons in this book and apply them to whatever situation you are in. Regardless of the scenario, you can be in control and ultimately decide who collects your private information.

Privacy is not dead. Thank you for reading.