# Personal Privacy for Professionals

Daniel Farber Huang
Theresa Menders

# Personal Privacy For Professionals

**Daniel Farber Huang**

**Theresa Menders**

Personal Privacy for Professionals
2022 Edition



Published by Princeton Studios

*For Quincy, Christian, Alexander and Celeste.*

Theresa Menders

*For* [redacted], [redacted], [redacted], [redacted], and [redacted]

*I* [redacted] *you.*

Daniel Farber Huang

Note: The chapters and sections highlighted in ORANGE are included in this preview.

# Contents

# Introduction

For every working professional, it's important to balance the demands of their income-generating, outward-facing, social persona against their irreplaceable, valuable private life.

Whether you are a rising associate or a C-level executive, separating and insulating your personal life from your public one is critically important so you can protect yourself, your loved ones, and the many non-work aspects of your life that you hold dear and precious. After all, what's the point of working so hard on our careers if we allow the personal aspects of our life to be harmed, violated, or exploited?

Personal Privacy for Professionals provides actionable strategies and practical tactics you can employ to protect your private life immediately.

We have helped numerous professionals who have been harassed, stalked, or threatened by disgruntled employees, internet trolls, online abusers, and anonymous threat actors. While those threat actors may have been triggered due to the victim's public or professional face, the abusers inevitably target or threaten the victim's private life because the abusers know that is where victims are most vulnerable and have the most to lose. In today's world, unfortunately, any working professional (and even retired professionals for that matter) may be vulnerable for the same type of unwelcome attention and abuse. What's even worse, many times the vitriol or anger that gets directed at a victim may not even have a triggering reason for occurring in the first place -- sometimes victims are targeted at random. Regardless of why, how, or when it occurs, we do know for a fact that victims never expect it to happen and are often blindsided when their privacy does get violated.

We want to prevent that from happening to you.

This book is based on the real-world experiences the authors have faced over the course of their professional corporate careers combined with their privacy and security expertise. Daniel Farber Huang Is a former investment banker, CEO, and strategy advisor on risk mitigation. Theresa Menders is a former investment banker, management consultant, and currently a senior director at a global pharmaceutical company. As a husband-and-wife team, Daniel and Theresa are also active humanitarian advocates and have learned to work in politically- or culturally-sensitive situations around the world. Daniel has traveled to 40 countries and Theresa to 50, and many of their privacy skills and strategies are the result of navigating through or around government bureaucracies (both domestic and international), military authorities, local police, and both organized and disorganized criminals. As frequent public speakers and journalists, the two have had to

ensure they maintain a carefully-curated public face while actively removing, obfuscating, or redirecting as much personal information from the internet and public records as possible.

Personal Privacy for Professionals covers both your physical world privacy and online privacy with clear, easy-to-understand directions that you can begin employing immediately. We intentionally avoid jargon or lengthy technical discussions and instead get to the guts of the matters fast. You're busy, we get it.

Our intention is to help you continue advancing in your career, which increasingly requires public visibility (at a minimum within your company and industry if not more broadly) while diligently protecting and separating the details of your private life from prying, potentially harmful eyes and threat actors who may seek to do you or your loved ones harm.

Since you've spent the last 60 seconds reading up to this point, we are going to infer that you have been thinking about privacy issues, likely your own but perhaps also that of people whom you care about. *Personal Privacy for Professionals* provides a comprehensive framework to give you significant control over your privacy, what information you choose to share with the outside world, and what information you choose to keep secure and protected. The goal of this book is to provide concise and actionable tactics, techniques, and procedures that you can employ.

We used to distinguish between the online world and the real world but that's not accurate anymore. There are online threats that are very real to their victims. There is such an overlap and merging of both worlds that in this book we have changed our terminology to the physical world and the online world. Some actions we discuss will protect you in the physical world while others protect you online. Because the line between our physical and digital worlds continues to narrow, it is imperative to take control of both sides.

Before getting into the technical details, it's important to point out that the greatest weakness to any security framework is the human element. Protections such as unlisted phone numbers, disposable credit cards, secure passwords or even out-of-state, physical mailing addresses can be arranged, but maintaining the integrity of such protections requires continued diligence and discipline. Think about treating your privacy the same way you would any other healthy habit, like exercising regularly or eating a balanced diet. Consistency is important for lasting results. Throughout this book, one common theme will be the importance of situational awareness and keeping your eyes open, trusting your instincts, and exercising your privacy mindset. While many of the topics we will cover might at first seem unfamiliar or even intimidating, we expect you will quickly become comfortable with enhancing your personal privacy framework through the pragmatic, no-nonsense, and measurable steps discussed here.

Daniel is Entrepreneur-in-Residence at CleanSlate.ai, which helps privacy-concerned individuals regain control of their personal privacy by compartmentalizing critical aspects of their life -- their public-facing persona, work life, private life – and putting the power back in their hands on what they share with whom. CleanSlate.ai helps clients shield themselves from the prying eyes and reach of data-hungry corporations, unfriendly influences, malicious actors, and other threats to personal privacy and safety. Many of the tactics, techniques, and procedures recommended in this book are drawn from CleanSlate.ai's privacy standards.

Daniel has worked closely with numerous federal, state, and local law enforcement agencies across the U.S. on providing solutions to their mobile technology requirements. He has focused on providing hardware and software solutions to federal field agents, investigators, the police, and other authorities to support them in performing their duties. Daniel is a strategic consultant helping a wide range of companies in different industries reduce risks at all levels of their organizations, including financial and cyber security. He has also worked with high-profile, C-suite executives on assessing the personal security frameworks for the executives and their families, including obfuscating their sensitive personal information, residences, and activities from the prying eyes of the public. Daniel earned his Master's degree in Journalism and Certificate in International Security from Harvard University. During his studies he has gained perspective and insight into the ways governments, non-state actors, corporations, and even lone individuals are using kinetic and cyberattacks not only against each other but also against unsuspecting civilians.

Theresa's privacy focus stems from both her career in the healthcare industry and her capabilities in public health and policy development. She is a Director at a thought-leading healthcare firm, where she has led critical corporate projects to align divisions with the organization's global strategic plans. Prior to that, Theresa was both a strategic consultant and investment banker for a wide range of clients ranging from entrepreneurial startups to global conglomerates. Beyond her corporate experience, Theresa attributes much of her ability to ask the right questions to broader experiences she has gained as a global explorer. Theresa understands firsthand how to navigate and thrive in rapidly shifting landscapes and uncertain environments. In the field, Theresa is notably accomplished in mobilizing scarce resources and negotiating cooperation from disparate stakeholders (from military authorities to law enforcement to NGOs to tribal leaders to local boots-on-the-ground personnel) to achieve mission objectives. Theresa is also a National Fellow of the Explorers Club, which promotes scientific inquiry in the natural world. Theresa is currently earning her PhD in Global Health from the University of Illinois. She earned her BS in Mathematics from Dartmouth College, MA in Latin American Studies and International Economics from Johns Hopkins University, and her MS in Global Health from George Washington University's Bloomberg School.

Finally, we both earned our MBAs from The Wharton School, University of Pennsylvania, where we were trained in efficiency so throughout this book we will get right to the point.

# Section I – The Privacy You Deserve

## Section Table of Contents

# Chapter 1 – The Privacy You Deserve

*NOTE: If you're in a rush and want to get to tactics immediately, jump to *Chapter 5: Action Plan Overview.* While these first 4 brief chapters are important to understand so you can run the rest of your strategies effectively, you can come back to them when you have a moment. We won't take it personally.

Today, our individual privacy is a rapidly diminishing resource. We have less and less of it as each hour and day passes by. Whether our privacy is violated due to intrusive information-gathering companies, government surveillance, nosy neighbors, ex-romantic partners, disgruntled employees, or internet trolls, our physical-world and digital or online lives provide abundant fields of information about our personal and professional lives. Oftentimes data is collected without our knowledge or permission, but just as commonly we may be freely offering our data when we click the Terms of Service agreements on the websites or apps we use. Depending on the circumstances, our private information may be getting stolen, aggregated, purchased, or left out in the wild through our own actions.

It's time to take back our information and control our privacy as much as possible. There are two ways to protect your privacy – proactively and reactively.

Sometimes bad circumstances descend upon us all at once and we are thrown into reactive mode, such as when internet trolls, stalkers, or other threat actors enter our lives. Those are bad situations, obviously, but they can still be managed. Those problems may not necessarily get fixed completely, but can still be managed as much as possible at that moment in time. If you are concerned about these types of issues, in this book we'll cover many actionable steps and strategies you can take immediately to control your privacy.

Other times, hopefully more common than not, we have the luxury of proactively taking steps to shore up our privacy protections. We'll cover a lot of that here too. Regardless of your current personal situation – whether you are under immediate threat or just beginning to determine your privacy comfort zone – there are actions you can take right now that can start building your personal privacy shields.

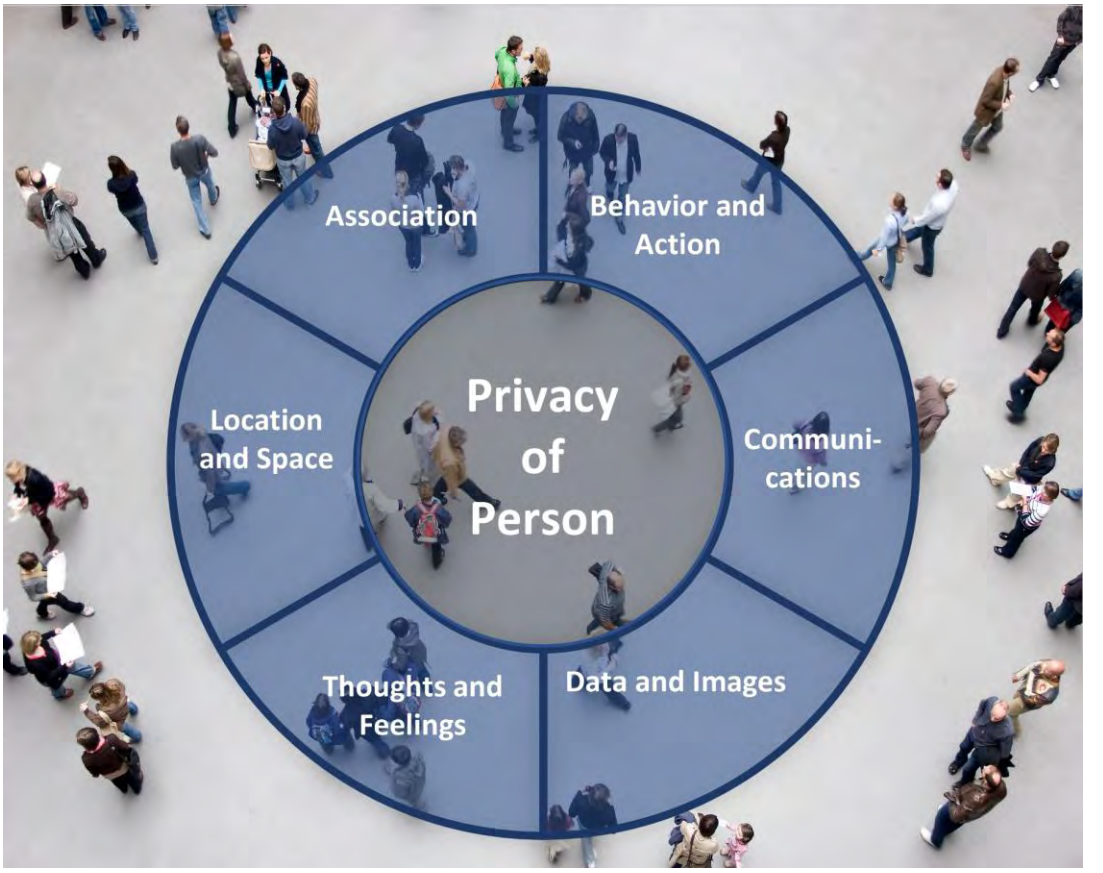
Before jumping into tactics and strategies, it's worthwhile to spend a moment and lay the groundwork about what we're actually trying to protect and from whom. The next few chapters are brief but important, because you want to protect your privacy for the long haul, not just for next month or until the end of the year, but rather you should aim to develop a consistent set of practices and a vigilant (but not overwhelmed) mindset where you are comfortably more alert about the orbits you occupy and the information you share.

It's worthwhile to take a step back and clarify what exactly about us we are seeking to preserve and protect.

There are several types of privacy, and we deserve autonomy over each one. In their publication, Seven Types of Privacy, the researchers Michael Friedewald, David Wright, and Rachel L. Finn identify these different categories of privacy.

You have a right to your privacy of:

1. Person,
2. Behavior and Action,
3. Communication,
4. Data and Images,
5. Thoughts and Feelings,
6. Location, and
7. Association




That's a lot of privacy we deserve! And each is worth protecting. More specifically…

**Privacy of Person** is the right to keep personal bodily functions and physical characteristics (such as genetic codes and biometrics) private.

**Privacy of Behavior and Action** includes sensitive issues such as sexual preferences and habits, political activities and religious practices.

**Privacy of Communication** aims to avoid the interception of communications, including mail interception, the use of bugs, directional microphones, telephone or wireless communication interception or recording and access to e-mail messages. Individuals benefit and society benefits from this aspect of privacy since it allows and encourages open discussion on a broad range of opinions and options.

**Privacy of Data and Images** expands on privacy of communication, and includes concerns about making sure that an individual's data is not automatically available to other individuals and organizations and that people can "exercise a substantial degree of control over that data and its use". The ability to control one's personal data builds self-esteem and empowers people.

**Privacy of Thoughts and Feelings** means people should be allowed to think and believe what they choose. This privacy is increasingly at risk from new and emerging technologies.

**Privacy of Location and Space** means that individuals have the right to move about in public or semi-public space without being identified, tracked or monitored. A right to seclusion, as well as a right to solitude in places such as the home, automobile, and workplace, is inherent in this notion of privacy.

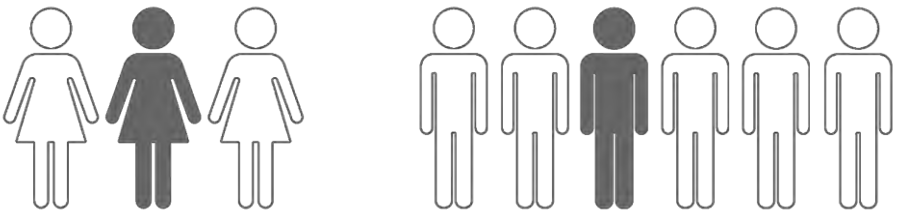
**Privacy of Association** (including group privacy) is concerned with people's right to associate with whomever they wish, without being monitored. This has long been considered essential and desirable for a democratic society since it promotes freedom of expression, including political speech, freedom of worship, and other forms of association.[1]

[1] Rachel L. Finn, David Wright, and Michael Friedewald, "Seven Types of Privacy," in *European Data Protection: Coming of Age*, ed. Serge Gutwirth et al. (Dordrecht: Springer Netherlands, 2013), 3–32, https://doi.org/10.1007/978-94-007-5170-5_1.

# Chapter 2 – Threats to Your Privacy

Every individual's privacy risk framework is unique, and there are many (too many) types of individuals or entities that may seek to violate a person's privacy and safety. To be able to protect your privacy, you need to know who or what you're protecting it from. Rather than lumping "bad guys" into one bucket, it's important to have an understanding of the different types of threats that may be encountered so you can determine which ones are most relevant to your situation.

About 1 in 3 women and 1 in 6 men have been stalked at some point in their lives.[2]



Let's briefly look at profiles of common threat actors, starting with the ones who may be physically closest to our personal circles and moving outward. Threat actors include:

- Different types of Stalkers;
- Poachers;
- Criminals;
- Organizations; and
- Governments.

[2] "Fast Facts: Preventing Stalking," Center for Disease Control, May 2, 2022, https://www.cdc.gov/violenceprevention/intimatepartnerviolence/stalking/fastfact.html.

## Stalkers

A stalker is a person who pursues someone obsessively and aggressively to the point of harassment and may be motivated for a number of reasons.

**Rejected stalkers** are the most common and dangerous type. They pursue the victim, often a former intimate partner, after a relationship ends. While many have desires for condolence and retribution, they often may feel a complicated and volatile combination of emotions.

**Intimacy-seeking stalkers** are obsessed with finding a lover they consider to be their "true love," and they tend to attribute their victims with particular desirability, excellence, and other qualities that correspond with their idea of romanticized love. Intimacy-seeking stalkers are typically not concerned with legal ramifications, seeing them as a necessary evil to achieve "real love."

**Incompetent stalkers** are aware that the victim is uninterested, but they continue to pursue her in the hopes of establishing a relationship. Stalking may be characterized as "crude" or "ineffective" attempts to court the target. Incompetent stalkers often are intellectually limited; they feel entitled to a partner but because of underdeveloped social skills are unable to build upon lesser forms of social interaction.

**Resentful stalkers** intend to frighten and distress the victim. They may pursue a revenge against a specific person or believe that the world is conspiring against them, leading them to select a victim at random. They frequently feel persecuted, and they may act with a sense of righteousness indignation in pursuit of their beliefs. Resentful stalkers stalk their prey to discover his or her weaknesses and seldom issue warnings, so the victim is generally ignorant of the danger.

**Predatory stalkers** are frequently afflicted with a pattern of recurring sexually arousing mental imagery or behavior that involves unusual and especially socially unacceptable sexual practices (known as paraphilias) and have a history of sexual offenses.[3]

**Political stalkers** are motivated by political beliefs and end up stalking people who either agree or disagree with their views. [4]

**Recreational stalkers** are a category we have been seeing increasing over the past several years where individuals or loosely coordinated groups of people on the internet choose to stalk a victim for sport. A different stalker or internet troll might have selected a victim and then broadcast a request among their community to target the victim.

---

[3] James Knoll, MD and Phillip J. Resnick, MD, "Stalking Intervention - Know the 5 Stalker Types, Safety Strategies for Victims," *Current Psychiatry* 6, no. 5 (May 2007).

[4] "7 Different Types of Stalkers | How To Identify a Stalker," *Fighter Law* (blog), March 17, 2020, https://www.fighterlaw.com/7-different-types-of-stalkers/.

Recreation stalkers may not necessarily care about the "reason" given to target a victim. Basically, recreational stalkers are assholes.

**Hitmen** are among the most dangerous stalkers as they have instructions, intention, and incentive to badly injury or murder a target.[5]

## Younger people are often targeted by stalkers[6]


## Poachers

We have added an emerging type of threat actor to our list in 2022: poachers, or individuals who target victims for state-sponsored monetary gain. With the overturn of Roe v. Wade and governments establishing bounty programs to persecute people seeking targeted healthcare services, individuals assisting those patients, or medical providers, poachers are people who persecute others for financial or other gain. For these definitions, poachers are differentiated from criminals because their actions are state-sponsored.

## Criminals

Criminals come in all shapes and sizes; may be organized or disorganized; local or international; young or old, you get the idea.

[5] "7 Different Types of Stalkers | How To Identify a Stalker."

[6] "Fast Facts."

## Organizations

There's a lot to unpack in this category, but simply put, organizations who may seek to do you harm may conduct one or more of these activities:

1. Gathering your information
2. Analyzing your information
3. Acting on your information
4. Benefiting from your information

Gathering can include the actions of data brokers (more on these companies in *Chapter 13 – Your Data for Sale*), hackers who steal account information, or any number of the countless legitimate businesses that collect your information (such as stores with frequent shopper accounts or tracking cookies) with the intention of data mining you further to make money off of you and your activities.

Analyzing groups include consulting firms, marketing firms, data scientists and others that want to take raw data and translate it into meaningful information, that can be used or sold.

Organizations that act on your information can range from grocery stores sending you targeted coupons (having previously analyzed your buying habits) to public relations firms trying to sway how you'll vote in elections to organized criminals that commit identity theft and other crimes using your information.

## Governments

It's worth clarifying that we are not anti-government or anti-police, but rather we are pro-privacy and pro-civil rights. We have great respect for the law enforcement officers and other public servants whose job it is to keep the public safe. We strongly believe that we as a society work better together when everyone can be accountable and responsible for their actions.

**U.S. Constitutional protections do not apply everywhere within the U.S.**

Government reach is wide and vast. Using the U.S. as an example (understanding that other nations have their own rules) basic U.S. Constitutional principles do not apply fully within an incredibly-wide boundary within U.S. borders.

U.S. Customs and Border Protection ("CBP"), the federal agency tasked with patrolling the U.S. border and areas that function like a border, claims a territorial reach much larger than you might imagine. A federal law says that, without a warrant, CBP can board vehicles and vessels and search for people without immigration documentation air up to 100 air miles from any external boundary of the U.S. The boundaries include international land borders but also the entire U.S. coastline.

Two-thirds of the U.S. population, or about 200 million people, reside within this expanded border region, according to the 2010 census. Most of the 10 largest cities in the U.S., such as New York City, Los Angeles, and Chicago, fall in this region. As illustrated in the below image some states, like Florida, lie entirely within this border band so their entire populations are impacted. [7]


Image credit: American Civil Liberties Union

[7] "Know Your Rights | 100 Mile Border Zone," *American Civil Liberties Union* (blog), https://www.aclu.org/know-your-rights/border-zone.

## Where is your information coming from?

Think about the many ways our personal information is vulnerable to being exposed, shared, archived, bought, and sold. And every single day more of our personal data is being compromised and exploited.

Appendix A provides exhaustive, illustrative lists of where our personal information may be exposed and who is collecting it. The objective of these lists is not to scare you (well, not too much at least) but rather to make you highly sensitive to how our seeming innocuous actions are creating data that is desirable to outsiders to sell, manipulate, track, spin, or otherwise try to exploit influence us and our actions.

The categories discussed provide examples of the many types of the physical world and digital information that can be gathered from our:

1. Homes;
2. Vehicles;
3. Computers;
4. Phones and Tablets;
5. Personal Habits;
6. Assets, Liabilities, Insurance, Legal;
7. Wallets and Purses;
8. Pets;
9. Genders and Ages;
10. Intimate Activities across the Gender Spectrum;
11. Academic;
12. Professional;
13. Identity; and
14. Community

Take a look.

**How many areas are you familiar with?**

**Are there any areas you haven't thought about lately?**


How and Where Is Your Information Being Collected?
NAME
Identity
Home
Community
Money
Personal Habits
Wallet
Computers
Vehicles
Mobile Devices
Pets
Intimate
Academic
Work

# Chapter 3 – Privacy Tactics, Techniques, and Procedures

Throughout this book, we will be discussing and recommending numerous tactics, techniques, and procedures to protect your privacy. It's helpful to spend a moment to clarify each of those terms.

A **tactic** is the highest-level description of an action or behavior, while **techniques** give a more detailed description of behavior in the context of a tactic, and **procedures** are highly detailed description of a technique.

There are several tactics that can be employed to increase privacy or reduce visibility and conspicuousness, and many can be used simultaneously depending on the circumstances. Some tactics may overlap as well (such as Diffusion and Dilution, which we discuss below). In any competition, understanding a variety of tactics builds your mental arsenal and makes you a more formidable opponent.

## Many People Have Little or No Privacy

### No Tactics = Minimal Privacy

Without employing any privacy tactics, you and your personal information are freely and readily available for other people or entities to observe, monitor, record, and analyze.

# Privacy Tactics to Employ

## Minimization = “need to know” basis

Minimization means sharing the minimum information necessary, whether it's with friends, businesses, or the general public. Sharing your home address only when absolutely required, keeping work like and home life separate, or not posting personal details on social media are examples of minimization.

## Obscurity = hiding, concealing

Obscurity means hiding or making yourself and your information difficult to observe or distinguish. The less information you show, the harder it is to obtain. Closing your window shades, using a VPN to hide your online activities, or wearing a face mask when outside are examples of obscurity.

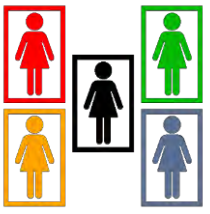
## Obfuscation = disinformation, fibbing, lying

Obfuscation means making something difficult to understand by being confusing and ambiguous. Using name variations for your package deliveries, providing a fake date of birth when signing up for a shopper rewards account at your grocery store, or using code words in communications are examples of obfuscation.

You can obfuscate the answer to a security question to prevent a hacker from impersonating you by making the answer something you identify with the subject in question, but not something obvious to outsiders. For example:

Security Question: What is your mother’s maiden name?
Obfuscated Answer: Rocky Road Ice Cream

## Compartmentalization = separate your different lives



By separating different aspects of your life, such as family, work, leisure, money matters, and keeping the relevant information for each aspect contained, it is harder for an observer (or stalker) to create a complete profile of you. Having separate computers for your work and personal use, maintaining an outward public persona while keeping your private life discrete, and using different emails for specific functions are examples of compartmentalization.

## Diffusion = blend in with the crowd, hide in plain sight

Diffusion means spreading something around, such as blending in with the crowd and not making yourself distinctive to target. When your information is sufficiently generic and the group over which it is collected is large enough, very little information can be attributed to a single individual, thus preserving your privacy. Going outside wearing nondescript clothing, not acting in a manner that would make you stand out from the crowd, and keeping a low profile are all ways of diffusing your identity.

## Dilution = make your information less concentrated

Dilution means making something less concentrated or powerful. Proving the last four digits of your social security number instead of all nine digits or telling someone, "Hi, I'm Inigo" instead of "Hello, my name is Inigo Montoya. You killed my father. Prepare to die,"[8] are examples of dilution.

## Distraction = "look over there!"

Distraction is different from obfuscation, as distraction seeks to divert a person's attention aware from an objective by interesting them in something else. Magicians, 3-card monte street hustlers, and some politicians are adept in using distraction in their lines of work.

## Randomness = apple, snowboarding, mermaid, Jupiter

All people are creatures of habit, which makes us predictable and therefore easy (or easier) to search for and track. Using different usernames when opening online accounts, varying your commuting route to work, and otherwise training yourself to be unpredictable all introduce randomness into your routines.

[8] *The Princess Bride* (Act III Communications, Buttercup Films Ltd., The Princess Bride Ltd., 1987).

# Identification Techniques

There are numerous ways our biometric information and behavioral characteristics can be used to identify us individually. It is also reasonable to expect new technologies will expand the existing list.

## Continued Privacy Requires Discipline

**Be alert = eyes up!**

It's easy to get distracted, whether that's by looking at our cellphones when we're out walking, being bombarded by too many incoming emails and not realizing the one we're about to reply to is a phishing attempt, or by multitasking. When someone knocks on your door make sure you don't let them in unless you are expecting them or they provide proper ID.[9]

**Be informed = know what is being asked of you**

You should make it a point to understand how your personal information is being used and stored. Be informed about which information is processed, for what purpose, and by which means. Use cases may be explicit, such as signing up for a certain service, or they might be implicit, such as walking into an area with video surveillance.

**Be in control = you decide**

The Control strategy is in fact an important counterpart to the Inform strategy. You should have control over how your personal data is handled. Data protection legislation sometimes gives us the right to view, update and even ask the deletion of personal data collected about ourselves. Pay attention to what is be asked of you.

**Enforce = hold others accountable**

Where possible, ensure that your privacy is being respected and handled by the outside party as they claim to be doing. Hold individuals and entities accountable, and stand up for yourself if they fail to act as promised.[10]

|

[9] "Distraction Burglary and Rogue Traders | Humberside Police," Humberside Police Department, https://www.humberside.police.uk/distraction-burglary-and-rogue-traders.

[10] Jaap-Henk Hoepman, "Privacy Design Strategies," *ArXiv:1210.6621 [Cs]*, May 6, 2013, http://arxiv.org/abs/1210.6621.

# Chapter 4 – Who Are YOU?

## Your Personally Identifying Information

Far beyond your name, address, date of birth, and Social Security number, be aware and protective of the significant amount of "other" information that exists out in the wild about you. The objective of these lists is not to scare you (well, not too much at least) but rather to make you highly sensitive to how your seemingly innocuous actions are creating data that is desirable to outsiders to sell, manipulate, track, spin, or otherwise try to influence us and our actions.

Below is a representative list of the types of personally identifying information that may exist about you, and where that information might be generated, collected, or found. Take a look. How many areas were you familiar with? How many hadn't you been aware of?

1. **Identification Basics**
    a. Age
    b. Citizenship
    c. Date of Birth
    d. Ethnicity / Race
    e. Full Name
    f. Gender
    g. Height
    h. Maiden name
    i. Nicknames
    j. Personal pronouns
    k. Personal style
    l. Photos
    m. Physical features
    n. Relationship status
    o. Sexual orientation
    p. Social media followers / following
    q. Usernames / Screennames
    r. Visual appearance (e.g., wardrobe, hairstyle, tattoos)
    s. Weight

2. **Identification - Aliases**
    a. Aliases - Pen Names
    b. Aliases - Physical world aliases
    c. Aliases - Usernames

3. **Identification - Signatures**
    a. Digitally signed
    b. Image scans
    c. Wet Signatures

4. **Identification - Miscellaneous**
    a. Digital avatars (e.g., gaming, social media)
    b. Digital identity

5. **Personal Physical Attributes**
    a. Biometric data - retina, face, fingerprints, handwriting, gait, typing, voice, speech

6. **Family**
    a. Adoption records
    b. Ancestry
    c. Birth announcements
    d. Mother's maiden name
    e. Obituaries (and bereavement marketers)
    f. Wedding announcements

7. **Affiliations**
    a. Endorsements (e.g., Facebook "Likes," "Dislikes")
    b. Memberships, frequent flyer #s, shopping cards

8. **Data Brokers**
    a. Credit agency reports
    b. Data brokers and directories

9. **Finances**
    a. Financial records

10. **Government**
    a. Criminal and arrest records
    b. Driver's license
    c. Government-issued ID
    d. Passport number
    e. Police reports
    f. Public records
    g. Social Security Number

h. Tax returns
i. Taxpayer ID number
j. Travel visas
k. Voting records

**11. Health**

a. Disability information
b. DNA (e.g., 23andMe)
c. Medical records
d. Patient identification number

**12. Insurance**

a. Health insurance claims
b. Health insurance policy
c. Life insurance claims
d. Life insurance policy
e. Property insurance claims
f. Property insurance policy

**13. Information Technology**

a. Deepfakes
b. Login credentials and passwords
c. Other people tagging you on social media

**14. Location**

a. Frequently visited locations
b. Geographical indicators
c. Home addresses
d. Location (country, state, city, street)
e. Place of birth
f. Previous residences, locations
g. Work addresses

# Chapter 5 – Action Plan Overview

*A good plan, even if poorly executed, is better than no plan.*

## Separate your Past and Present from your Tomorrow

When it comes to protecting (or ignoring) our personal privacy, we all have legacy actions, mistakes, slip ups, or things we forgot we did that have created the public footprint we have today. The past is past, so the best way to set our new and improved privacy framework is to separate our past (and today) from our tomorrow. Many of the strategies we suggest will be new, but many others may replace existing activities (such as your email accounts), which will require migrating accounts, subscriptions, or other elements to your new service providers over time. How fast you switch a resource and how pressing a particular change may be to protect you is often up to you.

In short, have no regrets, second thoughts, or doubts about the past. We move forward productively and intentionally from here.

# Set your priorities

Like with everything else in life, it's important not to get overwhelmed by what we want to accomplish. In practical terms, the philosophy that "done is better than perfect" applies here too.

Taking action can sometimes be intimidating and may place a person in unfamiliar territory and outside the normal boundaries of their comfort zone. We realize there is a lot of information included in this book and many tactics discussed. Our intention is to provide a thorough understanding of the possible strategies, recognizing that you will decide which ones are most important for your situation.

For each category covered, strategies are prioritized into three categories -- Levels 1, 2, 3. Level 1 are Urgent tasks that need to be done immediately. Level 2 are important but are less time-sensitive to accomplish. Level 3 tasks are non-critical, but nice to do if possible. In practice, we have found Leve 3 tasks often get pushed aside as progress is made and new, more refined Level 1 and 2 priorities emerge.

In a few chapters we include a Product Guide, which include discussion and possibly recommendations and for various tools, products or services that you may find suitable for your privacy concerns. We have used or tested many of these ourselves. You do not have to spend money on anything, but we do want to make you aware of various options should any be additive to your preparation. We might show a specific manufacturer or model in our illustrations, however, unless specifically noted we are agnostic on brand name or where you might purchase.

### Level 1 – Resilient Privacy Tactics

Urgent, do these as soon as practical. The results for some tactics may be immediate. Some others may take a longer period of time to become effective, but nevertheless should be considered in a timely manner.

### Level 2 – Practical Privacy Tactics

Important to consider, these tactics and tasks are generally less time sensitive than Level 1 to initiate. Level 2 tactics may require a greater amount of preparation or may be more specific strategies that may or may not be critical to your specific situation

### Level 3 – Supplemental Privacy Tactics

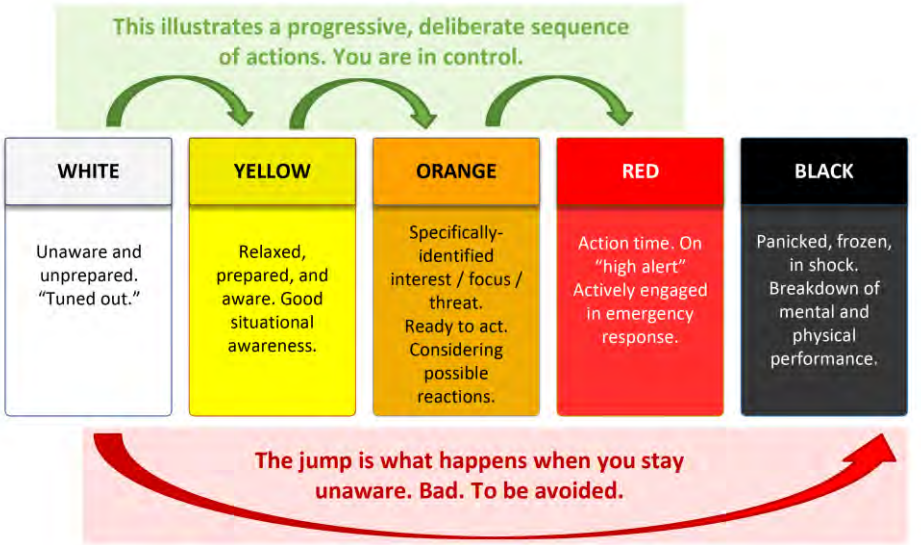
Non-critical yet valuable tactics to consider. Level 3 items are typically not time critical to complete.

### Product Guide

Tools, products or services that you may want to depending on your needs.

# Develop and Practice Situational Awareness

The human element is often the weakest link in your privacy goals. Being conscientious about what you're doing, and being aware of your current environment are healthy habits to develop, similar to maintaining good posture when walking. Jeff Cooper, a Major in the Marine Corps, developed what's known as Cooper's Colors, to illustrate situational awareness. Ideally, we would mentally progress to respond to a crisis.




**White**, the first stage, is how we are in our homes. We can tune out because that is our safe space.

**Yellow** is how we should be when we walk out the door. Still relaxed, but aware of our surroundings. Not staring at our cellphones when we walk, having a circle of awareness.

We enter **Orange** when we observe something and think "That's strange," or "That's odd," or even "That's interesting." We become ready to act, and consider possible reactions we might take.

**Red** is when action is required. You are actively engaged in your response.

If you practice situational awareness, you're better prepared to respond to uncomfortable situations in a measured and controlled manner, which is represented by the green arrow progression at the top of this slide.

If you stay in the white, unobservant, "tuned out" mode most of the time, you are going to miss the subtle cues that emerge as a situation escalates, which then can thrust you into the extreme, panicked stage (**Black**) where we become ineffective. Do not allow yourself to let that happen.

# Section 2 – Work / Life Balance

## Section Table of Contents

# Chapter 6 – Work and Professional Life

Every person who is employed by a company should understand there is no expectation of privacy in the workplace. Attorneys and experts on workplace-data collection say that companies are legally within their rights to gather information regarding employees' activities on the job. While on the surface that monitoring may seem perhaps slightly inconvenient but harmless, in reality the level of detail that can be monitored on employees can be incredibly intrusive.

## Level 1 – Resilient Work Privacy

### Use separate laptops for work and personal use

If you use a computer for work, if at all possible, we recommend you have a standalone, dedicated work computer (preferably provided by your company to save you the expense) and a separate personal computer that you own. It's too easy nowadays to cross-contaminate our online activities on whichever device might be close by and convenient, which merges our personal and work lives together more than they prudently should be.

Out of convenience, many smaller companies may have a lax technology policy that permits employees to conduct work activities on personal laptops or computers. Or larger companies may require employees use their IT-department issued devices. Either way, chances are many of us have used work computers for personal browsing, shopping, or emails, and others have used their personal computers for business tasks. Both habits should be stopped to protect your privacy.

Keep in mind that companies have every right to monitor their employees' online habits on company-issued devices. Furthermore, should a company be targeted with malware, spyware or other computer crime, you may be putting your personal information at risk if you use your personal device on company networks.

If you don't have a personal computer of your own, this should become a priority for you to acquire as it will be an important tool for much of your privacy implementation, as well as regular life activities.

Alternatively, if your work has not provided you with a company computer, speak to the appropriate person about needing a new laptop issued to you. If they say your work is important, they can afford it. If they balk at it, tell them your personal computer broke.

# JPMorgan Chase's tool collects data on everything employees do at work

According to a May 27, 2022 Insider article, JPMorgan Chase, America's largest bank, has developed a proprietary monitoring system that collects data on what hundreds of thousands of its bank employees are doing, from the moment they log into the company's workplace portal on their computers each day. The "Workforce Activity Data Utility," observes and documents everything from the length of employees' calls on Zoom or desk phones to the amount of time they spend actively using Microsoft Office applications like Outlook to draft emails or Excel to work on spreadsheets. Data from employees' company-issued BlackBerry cell phones and applications is also gathered. Many organizations use Big Data to draw broad-based conclusions about how workers spend their time or how best to accommodate their needs. Regulators like FINRA and the SEC require banks and brokerages to keep track of employees' workplace-related communication. "They can measure anything on your company BlackBerry," one person with knowledge said, such as phone calls, emails sent, or calendar information from the devices.

In addition to work-issued devices, personal cellphone activity has come under increased scrutiny in the regulated banking industry. The SEC recently ordered banks to hand over dozens of personal cellular devices to search for work-related messages that were possibly sent over noncompliant communications platforms. A former private-banking executive director disclosed he was instructed to download a communications-monitoring app named Movius onto his personal cellphone, which the bank uses to meet regulatory requirements. The executive was fine with downloading the app on a company-issued device, but was uncomfortable with the app's interface for personal use and refused to accommodate the directive for months. After being threatened with noncompliance, the employee installed the app on the personal device.

"There's no expectation of privacy in the workplace," said Helen Rella, an attorney and member of the global practice group at Wilk Auslander, a New York City-based law firm. "Indeed, when we're faced with situations involving employment termination or issues of improper use of confidential information, for example, we're able to have forensic experts come in, look at a computer that an employee has used, and track every keystroke that has ever transpired on that computer."

"If it's used relative to the workplace to determine if employees are actually working — which is what they're hired to do — then there's nothing impermissible about an employer monitoring the work that they are paying their employees to do," Rella added.[11]

[11] Reed Alexander, "Inside the Little-Known Tool That Gives JPMorgan Chase the Power to Collect Data about Everything Its Employees Do at Work," Business Insider,

## Use separate mobile phones for work and personal use

Similar to laptops, if your job requires you to communicate by cellphone to fulfill your duties, rather than use your personal cellphone for those tasks request your company issue you a separate device dedicated to work activities. Many companies offer employees a monthly phone reimbursement for using their personal cellphones, but it is significantly safer to use separate devices.

## Compartmentalize your work life from your personal life

Do not use work computers for personal internet browsing, emails, communications, shopping, data or document storage, or any other non-work-related activities. You should assume that everything you do on a work-issued computer, including every keystroke you make, is monitored, recorded, and stored for years. Some companies may be required by law to retain records for significant periods of time while others may store that information as a matter of policy. Memory and storage are inexpensive, and companies have access to lots of it. Also keep in mind that companies are not your friend, they are your employer. Their priority is protecting the company's interests, which may not be the same as protecting its people's best interests. If ever a contentious or litigious dispute were to arise between you and your employer, any information they have about you, your activities at work, and your duties might be reviewed in an adversarial light. Don't give them ammunition against you should a worst-case employer-versus-employee scenario ever arise.

Similarly, do not use work-issued mobile phones for personal calls, communications, browsing, app usage, games, or any other activities that are not related to your job and work responsibilities. Also do not use company landlines for personal calls. Most company landlines use Voice over Internet Protocol (otherwise known as VOIP), which is communication using an internet connection, and calls are easily recorded by VOIP systems. Assume that all landline calls are recorded and stored. Again, many regulated industries may be required to record communications (such as financial institutions) and others may record communications as a matter of policy.

If you do have to make personal calls during your work hours, use your personal cellphone. If you have to do personal computing during work hours, use your own laptop computer.

---

https://www.businessinsider.com/jpmorgan-chase-is-tracking-zoom-calls-workplace-activity-using-wadu-2022-5.

## Never use company WiFi for personal use

Never use company WiFi for personal use. Assume all internet traffic that uses company WiFi is recorded. If your laptop needs internet access for personal activities during work hours, use your mobile phone's hotspot to connect to the internet and not the company WiFi.

## No more LinkedIn recommendations

Try not to leave public reviews or referrals about people or companies you've interacted with. Don't leave roadmaps about where or with whom you have worked with in the past. If a threat actor has the time and determination to stalk you, you want to reduce the number of breadcrumbs that might lead back to you.

For example, let's say you left a professional review for a co-worker, manager, subordinate, colleague, associate, client, or friend on LinkedIn.com (for purposes of this discussion we'll call him Ringo) saying how highly you regard Ringo and their level of professionalism, blah blah blah. With moderately competent social engineering, a threat actor would be wise (even if nefarious) to call Ringo pretending to be perhaps a prospective client of yours or a hiring recruiter wanting to do a reference call about you. They could (and should) mention they read the glowing recommendation you left for Ringo on LinkedIn, so clearly Ringo should be able to give good insight into your work ethic and other details. Naturally, Ringo will want to be helpful (and earn brownie points from you) by elaborating on your many strengths to the caller. Those other details that can be uncovered over the course of a friendly conversation might include the company location where you work (if there are multiple facilities), who your clients are, where you often travel, where you are traveling next, what conferences or events you attend, your manager's name, and so on. What's more, if the stalker doesn't already have it, they might ask for your cellphone or work phone number, emails, and other contact information.

# Level 2 – Practical Work Privacy

## Change your mailing address

If you have set up an alternate local mailing address as discussed in *Chapter 8 – Your Home*, you should change your address in your employee records and have correspondence sent there. Employee data is not always secured properly from unauthorized access in the workplace, so there is no guarantee that a nosy co-worker will not be able to view your personal information through company systems. Your tax documents and other work-related mail should be sent to your alternate address.

## Remove your personal contact info from LinkedIn

Even if you don't make your email address or phone number publicly available on LinkedIn, but have in in your account information, there are readily available browser extensions that will reveal your contact information. These contact apps are often used by marketers or salespeople to generate leads, but can just as easily be used by stalkers. The best protection against this undesired access is to ensure your LinkedIn account only has your work phone number or a burner number, not your personal number. Similarly, use your work email as your primary address and your compartmentalized work-related email as the recovery email address.

Depending on your privacy needs, consider if it is necessary to display your actual work city or town in your LinkedIn profile, or could you list a different location as your base of operations.

## Don't believe your email

Phishing is rampant, and companies are targeted by threat actors from around the world. Be exceptionally wary of any email that does not come from a known associate, and written directly to you, not a form email. Lately we have been receiving emails from our IT Department stating an email has been quarantined, or a password is expiring, or other semi-urgent situation requiring attention. Only thing is, our small company does not have an IT Department (we call it something different), so the phishers have put together convincing emails that most certainly include a malicious link that, if clicked, would install perhaps spyware, a virus, ransomware, or some other malware.

## Be conscientious of small talk

Just because people may work with you, not everyone has earned the great privilege of your trust.

Depending on your privacy concerns and comfort level, you should decide in advance how much of your personal life you want to share with your work associates, whether they are your co-workers, clients, customers, or other contacts. It's human nature to want to share information and bond with other individuals, but sharing too

much with the wrong person can be disastrous. Taking it to an extreme, we know one senior professional who had experienced unpleasant situations with disgruntled co-workers at a prior company. Upon joining a new company, that manager made it a point to keep their personal life separate from their work life, and diligently avoided talking about their home life, family, or other topics of great personal importance. While that may be viewed by some as an extreme tact to take, that person was able to sleep well at night knowing they were proactively protecting their family.

## Videocall Safety

High resolution webcams can capture images in sharp detail. If your work involves videocalls, as many more do nowadays, be conscientious of the information you might unintentionally be sharing by the objects and decorations visible in your background. Consider blurring your background view or using a virtual background, both options should be available in your video settings.

Be aware that videocalls can be recorded both by the meeting organizer using the conference service and conference participants using basic capture apps on their own computers, without requiring permission from anyone. It's safe to assume that any of your videocalls might be recorded.

## Remove parking permits from your vehicle

As mentioned in *Chapter 9 – Your Vehicle*, if you are required to display a parking permit or other type of identification to park in a company parking lot, consider attaching your permit to something that can be removed from view when not needed so your work location or company is not readily visible to casual observers.

# Level 3 – Supplemental Work Tactics

## Job Search Safety Practices

Be conscientious when applying for jobs online. Increasingly, we are seeing company job postings requesting applicants to not only provide a resume and cover letter, but to also create applicant accounts on their job portals (often requiring you to re-type everything included in the resume – ugh!) and may request information on prior employment, including contact names and numbers of previous supervisors, job narrative or reasons for leaving, and also salary history. Understandably, a job seeker will want to make their application as attractive as possible and is therefore pressured to provide more information rather than less. Any company site is at risk of a data breach, and you don't want to share too much information if avoidable. Until you are hire, there are very few reasons to provide a social security number or date of birth. If a background check is required where you are asked for that or other sensitive information, use your judgment on when it's appropriate to share your data. Even if you are not providing a specific salary number, providing a high-low range of what you've earned previously or would like to earn in a new job can help criminals determine how attractive you might be to target.

Scammers have gone so far as to conduct phone or video interviews with applicants for fake job postings. Those interviews, of course, go swimmingly well, leaving the candidate excited about landing a coveted job. Then as part of their processing, the candidate is requested to provide their personal information, including scans of their driver's license and passport.

## Tighten up your LinkedIn Privacy Settings

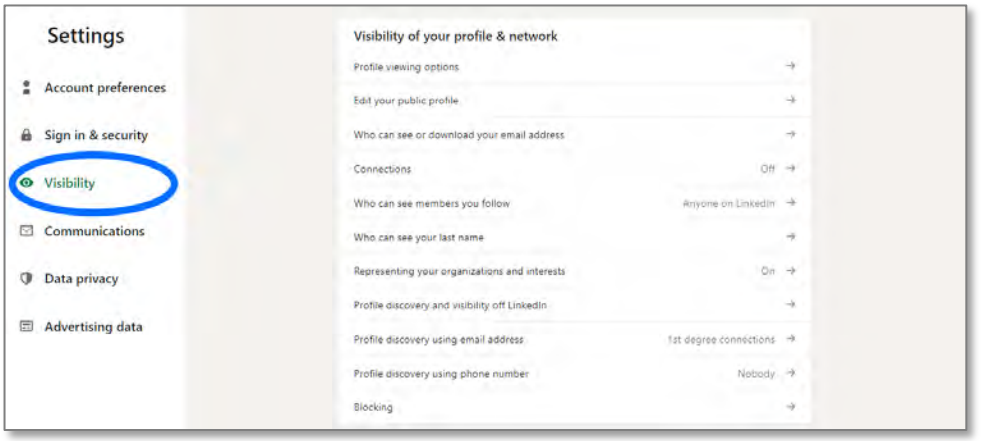
You should decide whom you want to share your email address with, not LinkedIn. If you have individual connections that are important to you, you'll have already given them your email or you can selectively choose to do so in the future. Keep your email private. If someone on LinkedIn wants to contact you, they can message you via LinkedIn. The last thing you need is for more solicitations from strangers arriving in your inbox.

**Tighten up your Sign in & Security settings**

You do not want data miners or strangers to obtain your personal email or phone number through LinkedIn channels. There are free browser extensions and apps that enable anyone to see the contact information in LinkedIn profiles, so you want to ensure your personal information is protected.

Under **Settings**, go to **Sign in & Security**. Set your email address to your **company email address**, and make your phone number your **work phone number**.

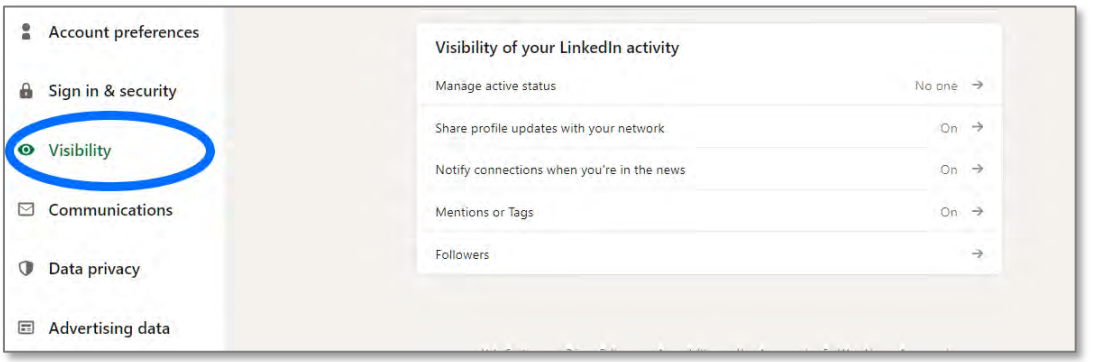

**Control your Visibility**




In **Settings**, go to **Visibility** and in the **Visibility of your Profile & Network** submenu, select the following:

- **Profile viewing options** – decide if you want your full profile or abbreviated profile displayed;
- **Edit your public profile** – check to ensure the information you choose to share in your public profile is there and any information you choose not to share going forward is removed;
- **Who can see or download your email address** – Only visible to me (i.e., You);
- **Connections** – do not allow connections to see your connections list, as it presents opportunity for too much cross-contamination of contacts;
- **Who can see members you follow** – Only visible to me;
- **Who can see your last name** – you decide if abbreviating your last name is helpful, although that information is already out in cyberspace;
- **Representing your organizations and interests** – Off, this is LinkedIn using you to advertise various activities, events, or companies you interact with;
- **Profile discovery and visibility off LinkedIn** – Off, this shares your profile to outside services;
- **Profile discovery using email address** – 1st degree connections;
- **Profile discovery using phone number** – Nobody, you don't want people using your phone number to search you out anywhere; and
- **Blocking** – you can block specific individuals from viewing you or contacting you here.

But wait, there's more…

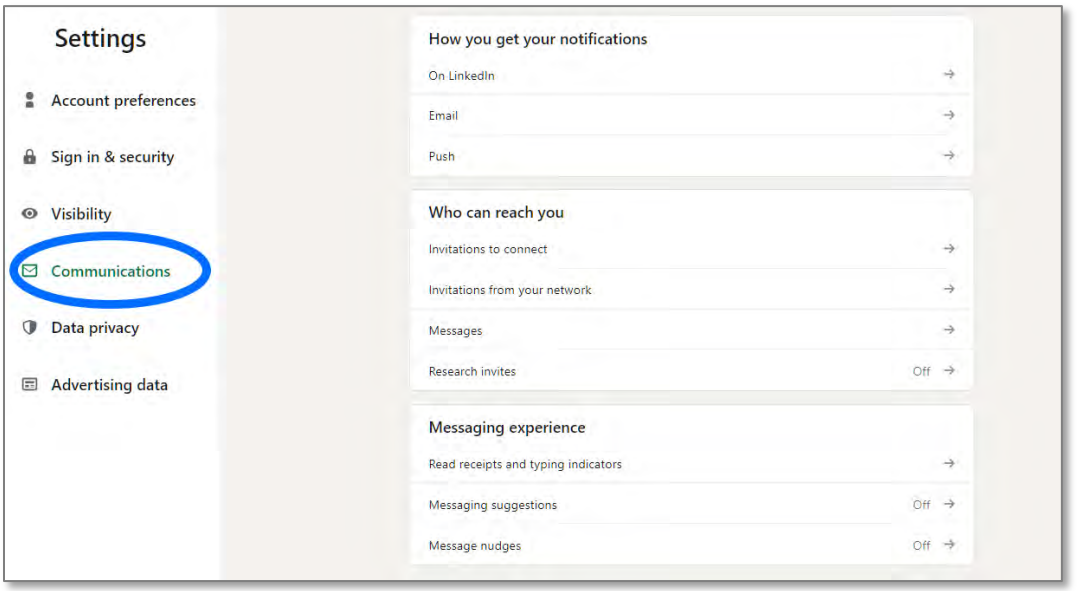



Still in the **Visibility** menu, scroll down to **Visibility of your LinkedIn Activity** and select:

- **Manage active status** – Set to No one, prevents people from seeing you are currently online;

- **Share profile updates with your network** – You can keep this On, this is the main function LinkedIn was originally intended to do: share your career progression with your network;
- **Notify connections when you're in the news** – On, same reason as above;
- **Mentions or Tags** – On; and
- **Followers** – You can choose either Everyone on LinkedIn or Your Connections depending on what's most useful for you.

**Set your Communications preferences**




Lots to turn off here, including:

In the submenu **How you get your notifications**, select:

- **On LinkedIn** – turn off as much as you can, only keep what's useful to your work;
- **Email** – turn Off all choices, it will only create more noise in your inbox; and
- **Push** – turn Off all choices.

In the submenu **Who can reach you**, select:

- **Invitations to connect** – you decide what's useful for your career;
- **Invitations from your network** – Off;
- **Messages** – you can say Yes to Message Requests and InMail Messages if helpful, and definitely turn off Sponsored Messages as it's more advertising; and
- **Research invites** – Off.

In the submenu **Messaging experience**, select:

- **Read receipts and typing indicators** – Off, people don't need to know what you are doing when;
- **Messaging suggestions** – Off; and
- **Message nudges** – Off.

**Fix your Data Privacy**

Data privacy typically is not something platforms hold sacred, so there's more to turn off here.

In the submenu How LinkedIn uses your data, select:

- **Manage your data and activity** – ignore this, LinkedIn made this function incredibly user-unfriendly so don't waste your time;
- **Get a copy of your data** – you should know this feature exists, but you'll probably never need it as the information will not be useful to you;
- **Manage cookie preferences** – turn all cookies Off;
- **Salary data on LinkedIn** – marketers would like this information, do not share any salary data;
- **Search history** – clear your search history and try to remember to clear it regularly;
- **Personal demographic information** – this section is a data broker's dream, so turn it Off and remove all personal demographics;
- **Social, economic, and workplace research** – Off;

In the submenu **Job seeking preferences**, select:

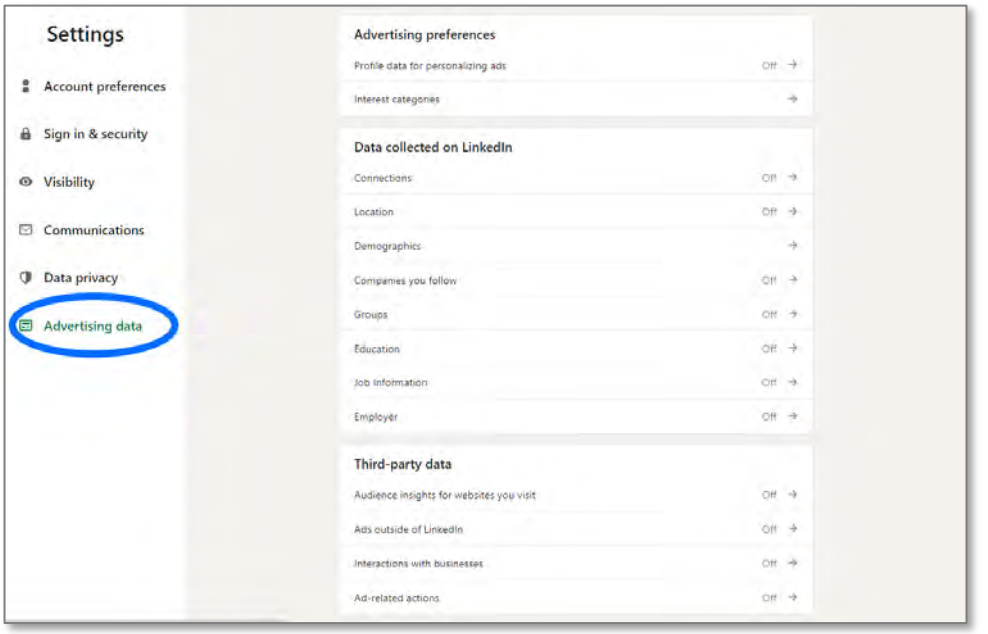
- **Job application settings** – Off;
- **Share your profile when you click Apply for a job** – Off;
- **Signal your interest to recruiters at companies you've created job alerts for** – Off;
- **Stored job applicant accounts** – delete.

In the submenu **Other applications**, select:

- **Permitted services** – do not grant access;
- **Microsoft Word** – okay, this one has a slight chance of being helpful if you ever use the Resume Assistant feature so leave it On if you like.

**Turn off all Advertising Data options.**

LinkedIn positions its advertising as being for your benefit. LinkedIn consistently mentions it can show you job advertisements, but does not discuss all the ways your valuable career data can be used for third party benefits. The downsides of having your data collected outweigh the upsides on social media platforms.




Turn off **Profile Data** sharing so LinkedIn doesn't data mine your company connections or content.


Turn off Interest Categories, so they don't data mine your profile or actions to advertise to you.

Turn off all Advertising Data settings on the Data Collected on LinkedIn submenu, including:

- **Connections;**
- **Location;**
- **Demographics;**
- **Companies You Follow;**
- **Groups;**
- **Education;**
- **Job Information;**
- **and Employer.**

Also turn off all Third-Party Data options, at the bottom of the Advertising Data settings menu, including:

- **Audience insights for websites you visit;**
- **Ads outside of LinkedIn;**
- **Interactions with businesses; and**
- **Ad-related actions.**

In all sincerity, we want to say Congratulations and even Thank You for getting this far through LinkedIn privacy control. The fact that this data removal process was so drawn out and tedious proves the point that websites and platforms collect massive amounts of information on each of us. Taking control can be an effort, but it is well worth it in both the immediate and long run.

## FBI Rap Back Program


It's helpful to be informed that law enforcement monitoring programs of this nature exist, which notify employers of any new (or previously unknown but now discovered) criminal history of their employees.

The FBI Noncriminal Rap Back Program notifies participating companies about changes to employees' criminal histories during their employment. When an individuals' fingerprints are submitted through an approved Next Generation Identification (NGI) connection and retained in the NGI System, an individual can be enrolled in a Rap Back Service. Once enrolled, the individuals' fingerprints will be subject to future searches in the NGI System. With Rap Back, an electronic notification will be generated if sometime later an applicant, employee, volunteer, or licensee engages in any criminal activity where fingerprints are taken and submitted to the NGI System. Companies will also be notified if any previously unreported criminal activity is updated to the Identity History Summary. Without Rap Back, employers depend on their employees to self-report their own criminal activity or have it discovered as a result of re-fingerprinting, possibly years later.

According to the FBI, the Rap Back Service can make a tremendous difference in the case of a nursing home employee arrested for selling stolen medications or a day care employee arrested for child pornography. It protects those served by coaches, teachers, law enforcement officers, and government employees.[12]

[12] "CJIS Noncriminal Rap Back Service," Video, Federal Bureau of Investigation, https://www.fbi.gov/video-repository/cjis-non_crim_rapback_2020.mp4/view.

# Chapter 10 – Case Studies in Photo Privacy

To illustrate how much subtle information photographs can reveal, here are some examples of what can be found in images people might post. Of course, there are a myriad of variations on what may be in a person's collection of photos across different social media accounts. Looking at a single photo may reveal elements of a person's information. A hacker, stalker, or troll would likely compile a range of clues from a target's accounts to compose a more comprehensive profile of that person's habits, interests, and activities.

For all the following examples, we use publicly available stock photos which are intended for commercial use. The individuals in the photos gave their respective photographers permission to use their images for publication. There is no intention to reveal personal information on any individuals in these photographs.

There is a tremendous amount of information that is freely available both on the internet and in the physical world, available for anyone to collect. This type of investigation is known as "open source intelligence gathering," or OSINT, and can be incredibly powerful.

An online stalker could easily magnify photos to search for details. In the following examples we will show different procedures for "pulling at threads" to unearth clues that can lead to valuable information. We will provide details on what closer inspection can reveal in each photo.

While Google is not great for protecting your personal privacy, their search tools otherwise are top notch for gathering data. Google Maps, including their Street View and Satellite View features, and Google Earth are extremely powerful tools to do reconnaissance, as you'll see in these examples. There are other search engines, such as Bing and DuckDuckGo that might catch items Google might have missed or might not has prioritized at the top of search results. Yandex is a Russian-originated search engine and sometimes has stronger capabilities for Eastern European topics.

The purpose of these next exercises is not to scare you into never posting photos, but to make you well aware of how images can be manipulated to work against your best and safest interests.

# Case Study #1

**Where was this photo taken?**

Photo by Alexa Suter for Unsplash

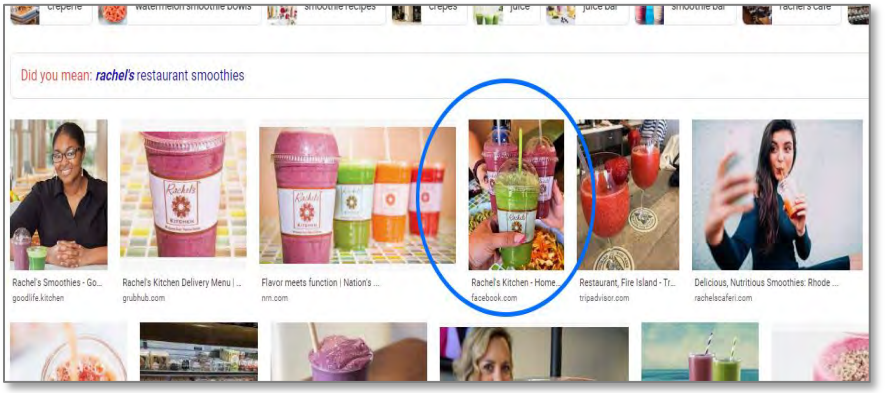
**Initial observations**

1. The woman is seated at an outdoor table on a sidewalk, likely eating lunch based on the food choice (a sandwich and fruit salad) and bright sunlight.
2. The small, round table has a green and gray tiled mosaic pattern, and the chair looks to be black metal with a curved back.
3. The drink in the plastic cup looks like a fruit smoothie. The name on the cup is blurry but looks like it says “Rachel’s.” The reflection on the drink’s plastic dome cover appears to show an evenly-spaced row of palm trees (based on their leaves) across the street, and a sunny sky.
4. The woman’s sunglasses are mirrored, and zooming in there appears to be a black stand or pillar of some sort with a black, square base.
5. The sidewalk immediately behind her appears to be gray, square bricks on her left side but cement on her right side.
6. There is a sidewalk sign in the background but too blurry to read.
7. Moving down the sidewalk, there appear to be three beige vertical elements followed by a red-brick colored vertical element in the closest building facades.

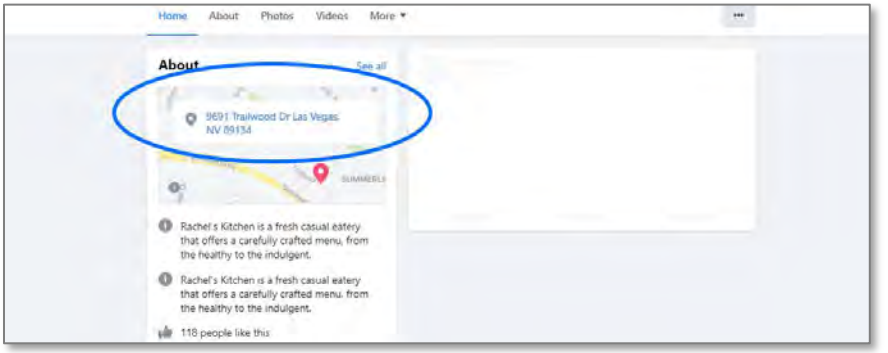
8. Cars in the background appear parked, possibly at an angle.
9. The trees in the background appear to be palm trees or something tropical based on their outer bark.

**Open Source Intelligence Gathering**

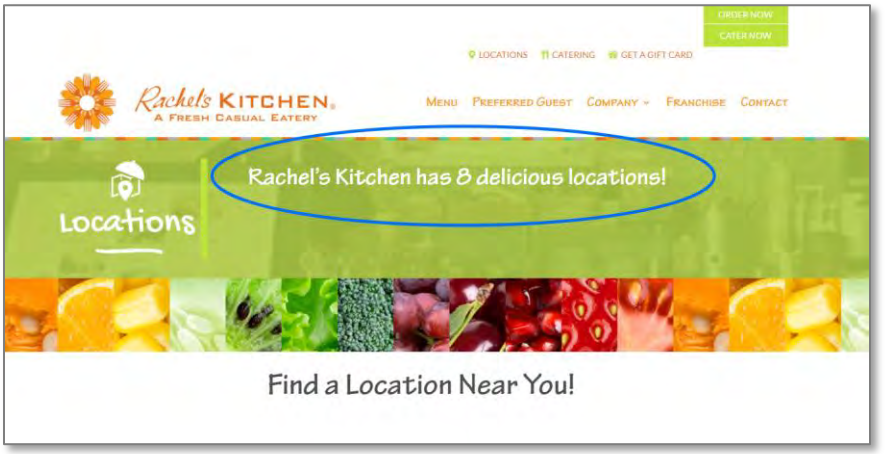
Assuming that the name on the drink was “Rachel’s” we Googled the search terms “rachels restaurant smoothies” then searched images. We quickly confirmed the cup’s name and logo was for Rachel’s Kitchen and found the restaurant’s Facebook page.



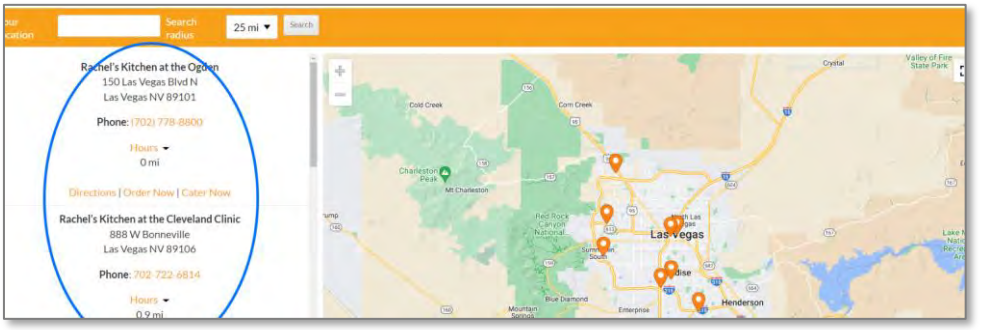

Their Facebook page showed a location in Las Vegas and their website address.




Rachel’s Kitchen’s website states they have eight locations, which is a relatively small number to search. Fortunately, Rachel’s Kitchen is not a national chain.



We obtained their addressed from their website and methodically searched each location using Google Street View. The first round of searches did not readily identify the location we were seeking. A second, more careful analysis did identify a potential match, which warranted further investigation.




Using Google Street View, we located the restaurant storefront.

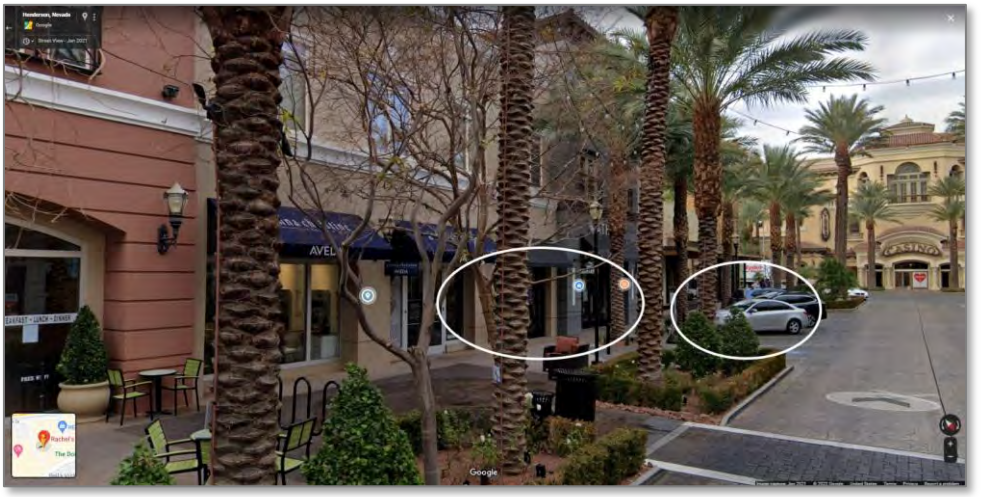

Unlike other locations we inspected, this location had similar tables as in the target photograph. The chairs were not the same.

Moving in closer, it would appear the woman was seated at the furthest-right table (since there were no tables visible behind her). The reflection in her sunglasses might be the bicycle stand but from this perspective the shapes do not match closely.


Moving to a different angle shows the bicycle stand has a square base similar to the sunglass reflection. Upon closer inspection of the sunglasses, it appears to be the same bicycle stand, however, the overhead sunlight casts a shadow that looked as if it were a solid part of the object.

We also see a clearer image of the sidewalk, which matches the target photo.

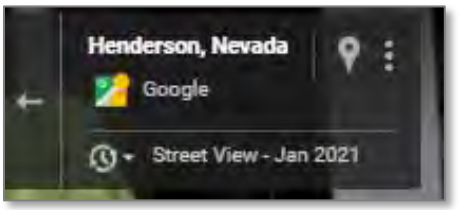
Looking down the street, we identified the three beige vertical elements in the nearest building façade. The following vertical elements are gray, and not the red-brick color in the target photo. We also see cars are parked at an angle to the sidewalk, similar to the cars in the photo.



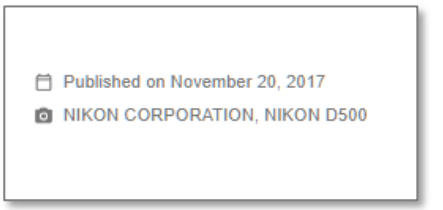

Upon closer inspection of the façade elements, we note that the horizontal architectural lines on the different facades line up at the bottom, similar to the lines in the target photo even though the colors are different.


We see the Google Street View is from January 2021. The metadata in the stock photograph indicates it was published in November 2017, so the photograph was taken on or before that date.

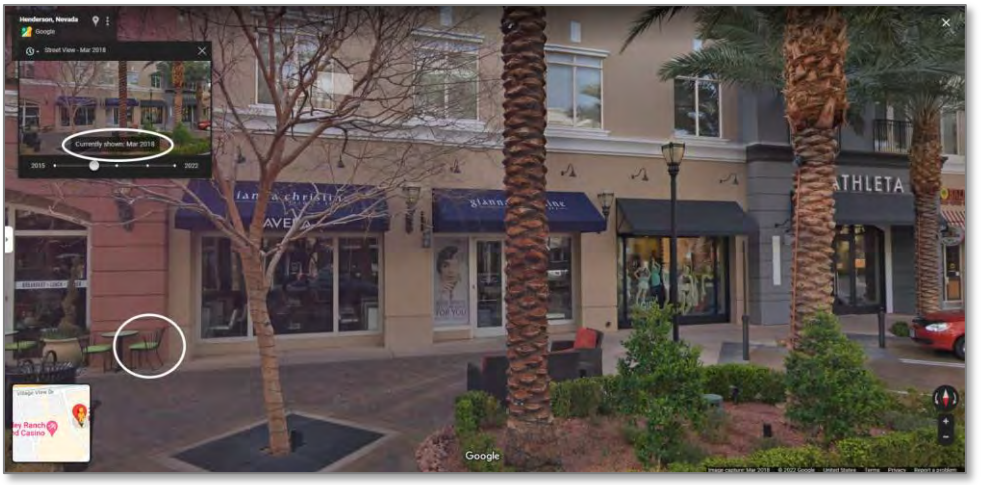
Date Google Street View Images were taken




Date photo was published on stock photo site



Google Street View allows you to look back in time to earlier Street View versions. Images from March 2018 still show the gray verticals. The chairs are different and match the chair in the target photo.




Images from April 2015, however, show the façade in question was colored red-brick, matching the target image.


There are several confirming elements using Google Street View to confirm this location is, in fact, the location where the target photo was taken.

# Concluding Thoughts

With enough time, effort, and determination, a person conducting an OSINT investigation can gather enormous amounts of information or “breadcrumbs” on a subject. Assembling those breadcrumbs into a reasonable, logical end-product or useful profile depends on the capabilities of the individual or team conducting the research. Using freely-available information and a methodical approach to researching observable pieces of information, we were able to identify the exact locations of two of the target photos, and gather additional information on the third photograph through a miniscule eye reflection.

Will a potential threat actor have reason or incentive to conduct similar reconnaissance on you today? We sincerely hope the answer is Hell No. But bear in mind that photos and information can stay on the internet forever so curating and controlling what information you put out into the wilds of cyberspace and social media is forever going to be important.

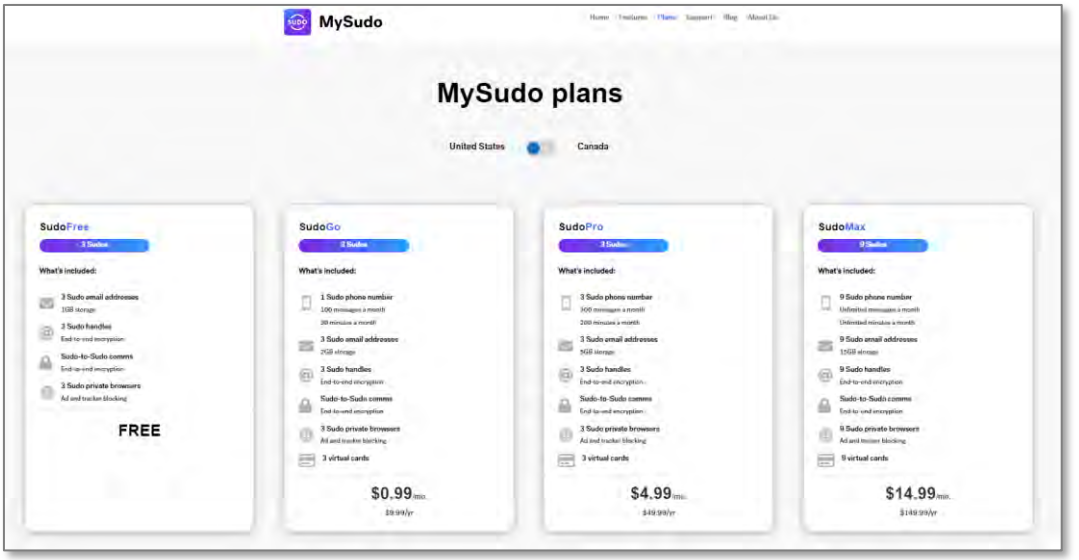
# Chapter 21 – Burner Phone Numbers

With our incredible reliance on our cell phones, having one private number for family and key relationships and separate phone numbers for the rest of the world can provide a buffer for your privacy. Rather than purchasing a second phone, burner phone apps can do the same job more affordably, sometimes requiring a monthly or annual fee but not requiring you to own a second device.

## MySudo phone numbers

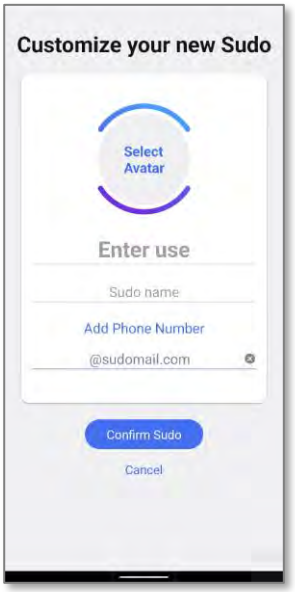
As part of developing a reliable framework for your different privacy tools, we recommend using MySudo for masked phone numbers.

MySudo's Pro plan offers three phone numbers, the Max plan offers nine numbers.

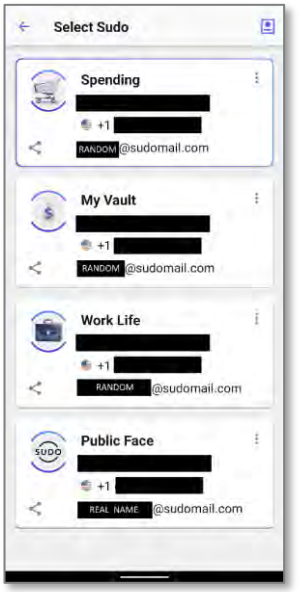



The following details the setup process:

**Step 1**
Install **MySudo** on your phone, choose the Pro or Max multi-phone plan

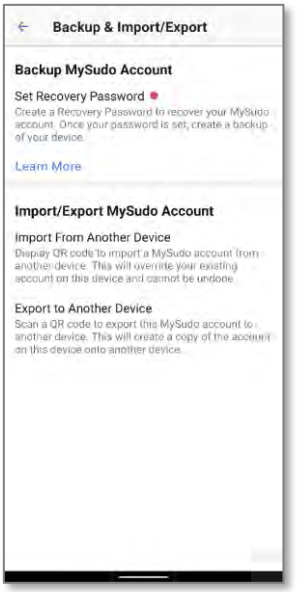



**Step 2**
Create your **profiles**. Use random email names except on your Public Facing email




**Step 3**

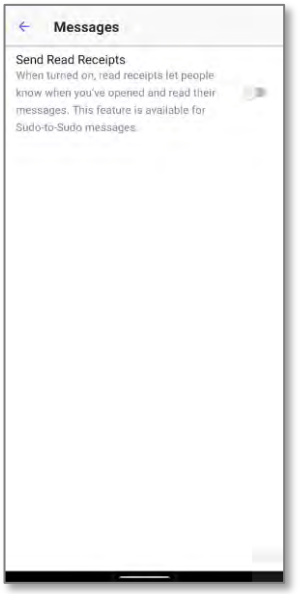
Create a **Recovery Password** and backup.



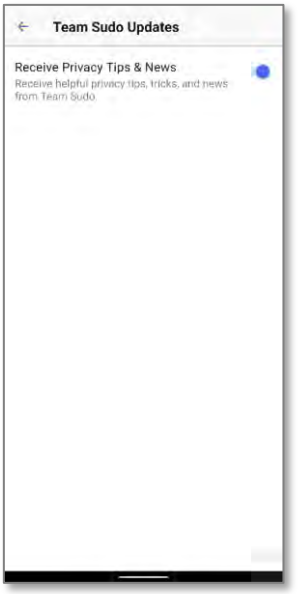

**Step 4**
Save your Recovery Password securely in your Password Keeper


**Step 5**

In the **Messages Setting**, turn of Read Receipts




**Step 6**
If helpful, turn on **Team Sudo Updates** to learn to use MySudo efficiently



## Other burner number options

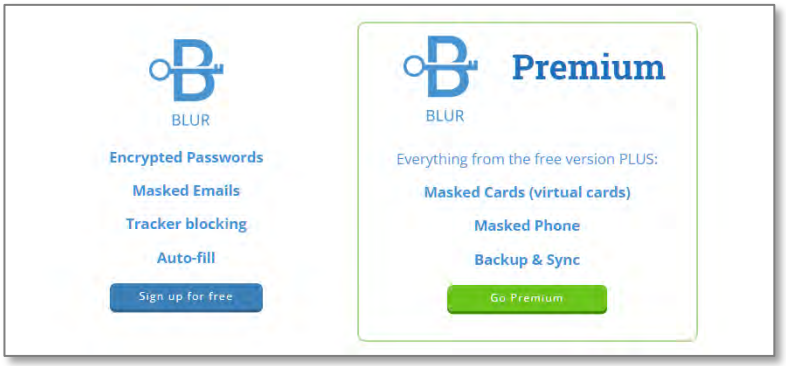
If you decide you want only one secondary number, in addition to Sudo's basic Go plan above, there are other providers you can consider for one additional phone line.

### Blur phone number

BLUR
Passwords, Payments, & Privacy

https://www.abine.com/

We use Blur's Premium plan (about $100 per year) for masked credit cards and disposable emails, and Premium also offers one phone number and a password keeper. If you aren't set up with a password keeper yet or will have need of masked credit cards (more of this in *Chapter 20 – Money Matters*) using Blur might address several of your privacy needs. Blur is run by the same company, Abine, that manages the DeleteMe data broker removal service. Their Blur interface is sort of ugly and inelegant, but it works well for our needs.



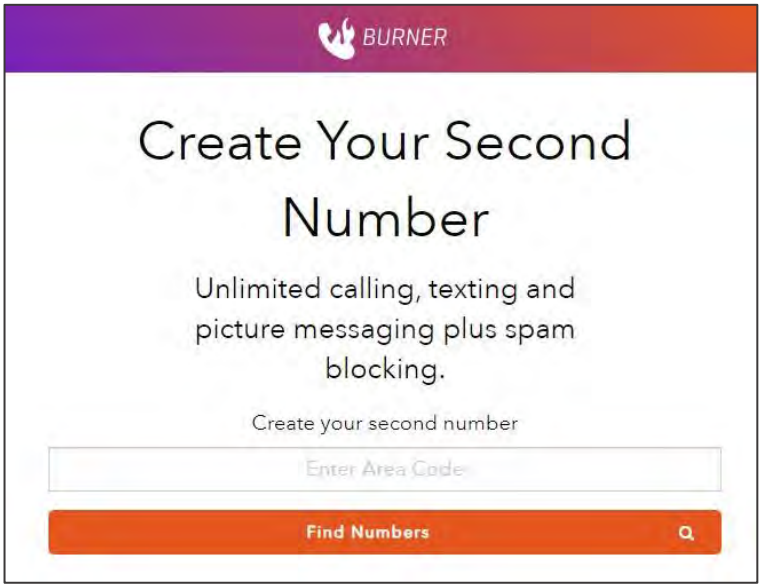

### Google Voice

Google Voice will provide you with a free phone number through its app. Because it's from Google, it's not great for privacy but it is free so can be used as a "starter" spare number. Google Voice is not anonymous.

Two other paid apps you could consider are Burner and Hushed.

**Burner App**

https://www.burnerapp.com/




**Hushed App**

https://hushed.com/

# About the Authors

**Theresa Menders** is an experienced corporate strategist with a successful track record of building and scaling companies across a wide range of industries. Theresa has worked in in-depth operations, program management, strategic consulting and corporate finance with a primary focus on managing complex, multi-faceted growth initiatives with organizations ranging from global conglomerates to startups. Theresa is a Director at a thought-leading healthcare firm, where she has led critical corporate projects to align divisions with the organization's global strategic plans. She has worked in various roles and departments throughout the company from conducting long-range program planning and agile execution and ensuring the strategic execution of business priorities for human resources to leading strategic and operational planning for information technology, while managing annual budgets ranging from $5 million to $60 million.

Theresa's earlier experience includes Merrill Lynch Investment Banking, where she executed mergers and acquisitions deals, cross-border transactions and institutional capital raising. She also worked at Mercer Management Consulting, where she advised U.S. and international companies on global expansion and implementation strategies.

Theresa is currently earning her Doctorate in Public Health from the University of Illinois, Chicago School of Public Health. She earned her BA in Mathematics from Dartmouth College, MBA in Finance and Management from The University of Pennsylvania's Wharton School, MA in Latin American Studies and International Economics from Johns Hopkins University's School for Advanced International Studies, and her Master in Public Health from George Washington University's Milken Institute School of Public Health.

**Daniel Farber Huang** is a strategic consultant and advisor on cyber security and other risk mitigation issues to a broad array of companies and organizations, ranging from entrepreneurial start-ups to multi-national corporations. He has worked closely with

numerous federal, state, and local law enforcement agencies across the U.S. on providing solutions to their mobile technology requirements. Daniel has focused on providing hardware and software solutions to federal field agents, the police, and other authorities to support them in fulfilling their duties.

Daniel is Entrepreneur-in-Residence of CleanSlate.ai, which helps privacy-concerned individuals regain control of their personal privacy by compartmentalizing critical aspects of their life -- their public-facing persona, work life, private life – and putting the power back in their hands on what they share with whom. Clean Slate helps clients shield themselves from the prying eyes and reach of data-hungry corporations, unfriendly influences, malicious actors, and other threats to personal privacy and safety.

Before founding his own independent advisory firm, Daniel worked for Goldman, Sachs & Co., Merrill Lynch and other major investment banks advising a corporations and investors on domestic and international corporate finance transactions. He was actively involved in capital raising engagements encompassing in excess of $10 billion. Daniel has advised a wide range of investment sponsors and strategies, including private equity, venture capital, infrastructure, real estate, emerging markets, hedge funds and specialized situations. Daniel is an Advisor to Princeton University's Keller Center for Innovation in Engineering Education, where he advises startups founders on business best practices.

Daniel earned his Master's degree (A.L.M.) in Journalism and a Certificate in International Security from Harvard University, an M.B.A. from The Wharton School, University of Pennsylvania in Finance and Entrepreneurial Management, and a B.A. from New York University in Economics.

# Bibliography


Alexander, Reed. “Inside the Little-Known Tool That Gives JPMorgan Chase the Power to Collect Data about Everything Its Employees Do at Work.” Business Insider, n.d. https://www.businessinsider.com/jpmorgan-chase-is-tracking-zoom-calls-workplace-activity-using-wadu-2022-5.

Amazon.com. “Door Lock for Home Security,” n.d. https://www.amazon.com/gp/product/B08B35YC3C/ref=ppx_yo_dt_b_search_asin_title?ie=UTF8&psc=1.

Amer, Pakinam. “Deepfakes Are Getting Better. Should We Be Worried?” Boston Globe, December 13, 2019. https://www.bostonglobe.com/2019/12/13/opinion/deepfakes-are-coming-what-do-we-do/.

American Civil Liberties Union. “Know Your Rights | 100 Mile Border Zone,” n.d. https://www.aclu.org/know-your-rights/border-zone.

American Civil Liberties Union. “The United States Bill of Rights: First 10 Amendments to the Constitution,” n.d. https://www.aclu.org/united-states-bill-rights-first-10-amendments-constitution.

Angwin, Julia. “How Journalists Fought Back Against Crippling Email and Subscription Bombs.” WIRED, November 9, 2017. https://www.wired.com/story/how-journalists-fought-back-against-crippling-email-bombs/.

Anon, Dennis. “How Cookies Track You around the Web & How to Stop Them.” Privacy.Net (blog), February 24, 2018. https://privacy.net/stop-cookies-tracking/.

Anonymous. “How a Group of Online Misogynists Tried to Ruin My Professional Life.” Women’s Media Center (blog), March 31, 2016. https://womensmediacenter.com/speech-project/how-a-group-of-online-misogynists-tried-to-ruin-my-professional-life.

Avery, Dan. “Your Social Security Number: When Is It Safe to Share It?” CNET, n.d. https://www.cnet.com/how-to/your-social-security-number-when-is-it-safe-to-share-it/.

Ayyub, Rana. “I Was The Victim Of A Deepfake Porn Plot Intended To Silence Me.” Huffington Post UK, November 21, 2018. https://www.huffingtonpost.co.uk/entry/deepfake-porn_uk_5bf2c126e4b0f32bd58ba316.

Bazzell, Michael. Extreme Privacy: What It Takes to Disappear in America. Independently published, 2019.

BBC News. “Cyber Attacks Briefly Knock out Top Sites,” October 21, 2016. https://www.bbc.com/news/technology-37728015.

BBC News. “Punctuation Protest against Far Right Trolls on Twitter,” June 8, 2016, sec. Trending. https://www.bbc.com/news/blogs-trending-36470879.

Bibliography

Bradford, Alina. “8 Red Flags Someone’s Tracking Your Cell Phone.” Reader’s Digest, September 26, 2020. https://www.rd.com/article/red-flags-someones-tracking-your-cell-phone/.

Brodkin, Jon. “Tim Hortons Coffee App Broke Law by Constantly Recording Users’ Movements.” Ars Technica, June 2, 2022. https://arstechnica.com/tech-policy/2022/06/tim-hortons-coffee-app-broke-law-by-constantly-recording-users-movements/.

Center for Disease Control. “Fast Facts: Preventing Stalking,” May 2, 2022. https://www.cdc.gov/violenceprevention/intimatepartnerviolence/stalking/fastfact.html.

Center for Disease Control. “Stalking Awareness Month,” January 8, 2021. https://www.cdc.gov/injury/features/prevent-stalking/index.html.

Chandler, Daniel, and Rod Munday. “Sealioning.” In A Dictionary of Social Media, 2016th ed. Oxford University Press, 2016. https://www.oxfordreference.com/view/10.1093/acref/9780191803093.001.0001/acref-9780191803093-e-1257.

Childnet International. “About Project DeSHAME,” n.d. http://www.childnet.com/our-projects/project-deshame/about-project-deshame.

Committee to Protect Journalists. “Digital Safety: Protecting against Targeted Online Attacks,” September 28, 2020. https://cpj.org/2020/05/digital-safety-protecting-against-targeted-online-attacks/.

Committee to Protect Journalists. “Psychological Safety: Online Harassment and How to Protect Your Mental Health,” September 4, 2019. https://cpj.org/2019/09/psychological-safety-online-harassment-emotional-health-journalists/.

Consumer Reports. “30-Second Privacy Fixes: Simple Ways to Protect Your Data,” n.d. https://www.consumerreports.org/privacy/30-second-privacy-fixes-simple-ways-to-protect-your-data-a9402343475/.

Consumer Reports. “New ‘Off-Facebook Activity’ Reveals How Company Tracks You All Across the Web,” n.d. https://www.consumerreports.org/privacy/off-facebook-activity-clear-history-data-collection-a3690858466/.

Cyber Civil Rights Initiative. “46 States + DC + One Territory NOW Have Revenge Porn Laws,” n.d. https://www.cybercivilrights.org/revenge-porn-laws/.

Cyber Civil Rights Initiative. “Definitions,” n.d. https://www.cybercivilrights.org/definitions/.

Cyberbullying Research Center. “What Is Cyberbullying?,” December 23, 2014. https://cyberbullying.org/what-is-cyberbullying.

Elder, Miriam. “Hacked Emails Allege Russian Youth Group Nashi Paying Bloggers.” The Guardian, February 7, 2012, sec. World news. http://www.theguardian.com/world/2012/feb/07/hacked-emails-nashi-putin-bloggers.

Farkas, Brian. “Child Photography or Videotaping Consent Laws,” May 27, 2020. https://www.lawyers.com/legal-info/personal-injury/types-of-personal-injury-claims/child-photography-or-videotaping-consent-laws-are-changing.html.

Federal Bureau of Investigation. “CJIS Noncriminal Rap Back Service.” Video, n.d. https://www.fbi.gov/video-repository/cjis-non_crim_rapback_2020.mp4/view.

Federal Bureau of Investigation. “Cyber Crime,” n.d. https://www.fbi.gov/investigate/cyber.

Fighter Law. “7 Different Types of Stalkers | How To Identify a Stalker,” March 17, 2020. https://www.fighterlaw.com/7-different-types-of-stalkers/.

Filipovic, Jill. “Let’s Be Real: Online Harassment Isn’t ‘Virtual’ For Women.” Talking Points Memo, January 10, 2014. https://talkingpointsmemo.com/cafe/let-s-be-real-online-harassment-isn-t-virtual-for-women.

Finn, Rachel L., David Wright, and Michael Friedewald. “Seven Types of Privacy.” In European Data Protection: Coming of Age, edited by Serge Gutwirth, Ronald Leenes, Paul de Hert, and Yves Poullet, 3–32. Dordrecht: Springer Netherlands, 2013. https://doi.org/10.1007/978-94-007-5170-5_1.

Fleishman, Cooper, and Anthony Smith. “‘Coincidence Detector’: The Google Chrome Extension White Supremacists Use to Track Jews.” Mic, June 2, 2016. https://www.mic.com/articles/145105/coincidence-detector-the-google-extension-white-supremacists-use-to-track-jews.

Friedberg, Brian, Gabrielle Lim, and Joan Donovan. “Space Invaders: The Networked Terrain of Zoom Bombing.” Technology and Social Change Research Project, June 9, 2020. https://doi.org/10.37016/TASC-2020-02.

Germain, Thomas. “How to Protect Phone Privacy and Security During a Protest.” Consumer Reports, June 3, 2020. https://www.consumerreports.org/privacy/protect-phone-privacy-security-during-a-protest/.

Google Support. “Maps User Contributed Content Policy: Privacy,” n.d. https://support.google.com/contributionpolicy/answer/7401426?hl=en&ref_topic=7422769.

Guariglia, Matthew. “Ring Changed How Police Request Door Camera Footage: What It Means and Doesn’t Mean.” Electronic Frontier Foundation, June 7, 2021. https://www.eff.org/deeplinks/2021/06/ring-changed-how-police-request-door-camera-footage-what-it-means-and-doesnt-mean.

———. “Senator Declares Amazon Ring’s Audio Surveillance Capabilities ‘Threaten the Public.’” Electronic Frontier Foundation, June 14, 2022. https://www.eff.org/deeplinks/2022/06/senator-declares-concern-about-amazon-rings-audio-surveillance-capabilities.

HeartMob. “Join the Movement to End Online Harassment,” n.d. https://www.iheartmob.org.

HG.org Legal Resources. “Bounds of Privacy in Public Locations -- What Is Legal? - HG.Org,” n.d. https://www.hg.org/legal-articles/bounds-of-privacy-in-public-locations-what-is-legal-35724.

Hoepman, Jaap-Henk. “Privacy Design Strategies.” ArXiv:1210.6621 [Cs], May 6, 2013. http://arxiv.org/abs/1210.6621.

HTML.com. “What Is Doxing? (And Why Is It So Scary?): An Infographic,” n.d. https://html.com/blog/doxing/.

Humberside Police Department. “Distraction Burglary and Rogue Traders | Humberside Police,” n.d. https://www.humberside.police.uk/distraction-burglary-and-rogue-traders.

Identity Theft Resource Center. “Identity Theft: The Aftermath Study,” n.d. https://www.idtheftcenter.org/identity-theft-aftermath-study/.

Internal Revenue Service. “Questions and Answers about Reporting Social Security Numbers to Your Health Insurance Company,” n.d. https://www.irs.gov/affordable-care-act/questions-and-answers-about-reporting-social-security-numbers-to-your-health-insurance-company.

Jacobsen, Jenni. “25 Tips to Stay Safe When an Ex Becomes a Stalker.” Marriage.com, February 23, 2022. https://www.marriage.com/advice/relationship/tips-to-deal-with-a-stalker-ex/.

Jacobson, Roni. “I’ve Had a Cyberstalker Since I Was 12.” WIRED, February 29, 2016. https://www.wired.com/2016/02/ive-had-a-cyberstalker-since-i-was-12/.

Jeffries, Adrianne. “Meet ‘swatting,’ the Dangerous Prank That Could Get Someone Killed.” The Verge, April 23, 2013. https://www.theverge.com/2013/4/23/4253014/swatting-911-prank-wont-stop-hackers-celebrities.

Keheley, Paulette. “How Many Pages In A Gigabyte? A Litigator’s Guide.” Digital WarRoom (blog), April 2, 2020. https://www.digitalwarroom.com/blog/how-many-pages-in-a-gigabyte.

Kessler, Sarah. “Why Online Harassment Is Still Ruining Lives–And How We Can Stop It.” Fast Company, June 3, 2015. https://www.fastcompany.com/3046772/why-online-harassment-is-still-ruining-lives-and-how-we-can-stop-it.

Knoll, MD, James, and Phillip J. Resnick, MD. “Stalking Intervention - Know the 5 Stalker Types, Safety Strategies for Victims.” Current Psychiatry 6, no. 5 (May 2007).

Kushner, David. “‘We Have Your Daughter’: The Terrified Father Paid the Ransom. Then He Found His Kid Where He Least Expected Her.” Business Insider, n.d. https://www.businessinsider.com/virtual-kidnappers-scamming-terrified-parents-out-of-millions-fbi-2022-3.

Legal Information Institute. “18 U.S. Code § 2261A - Stalking,” n.d. https://www.law.cornell.edu/uscode/text/18/2261A.

Lexico Dictionaries. “Definition of Threat,” n.d. https://www.lexico.com/en/definition/threat.

Lorenz, Taylor. “‘Zoombombing’: When Video Conferences Go Wrong.” The New York Times, March 20, 2020, sec. Style. https://www.nytimes.com/2020/03/20/style/zoombombing-zoom-trolling.html.

Lucas, Suzanne. “When an Employer Can--and Can’t--Ask for a Social Security Number.” Inc.com, February 25, 2020. https://www.inc.com/suzanne-lucas/when-an-employer-can-and-cant-ask-for-a-social-security-number.html.

Morris, David Z. “Bestselling Feminist Author Jessica Valenti Quits Social Media After Rape and Death Threats Directed at Daughter.” Fortune, July 31, 2016. https://fortune.com/2016/07/31/bestselling-feminist-author-jessica-valenti-quits-social-media-after-rape-and-death-threats-directed-at-daughter/.

Mozilla. “Seven of the Best Browsers in Direct Comparison,” n.d. https://www.mozilla.org/en-US/firefox/browsers/compare/.

National Crime Victim Law Institute. “What Are the Differences between the Civil and Criminal Justice System?,” n.d. https://law.lclark.edu/live/news/5497-what-are-the-differences-between-the-civil-and.

National Public Radio. “Jewish Reporters Harassed By Trump’s Anti-Semitic Supporters,” July 6, 2016. https://www.npr.org/2016/07/06/484987245/jewish-reporters-harassed-by-trumps-anti-semitic-supporters.

Nguyen, Audrey, and Noel King. “If You’re Stopped By Police, You Have Rights To Protect You. Here’s What To Remember.” National Public Radio, October 28, 2020, sec. Life Kit. https://www.npr.org/2020/10/23/927134939/if-youre-stopped-by-police-you-have-rights-to-protect-you-here-s-what-to-remembe.

Palmer, Jordan. “OnePlus Nord N20 5G Review: The Best Phone under $300.” Tom’s Guide, June 27, 2022. https://www.tomsguide.com/reviews/oneplus-nord-n20-5g.

Pascual, Al, and Kyle Marchini. “2018 Child Identity Fraud Study.” Javelin, April 24, 2018. https://www.javelinstrategy.com/coverage-area/2018-child-identity-fraud-study.

PEN America, Online Harassment Field Manual. “Defining ‘Online Abuse’: A Glossary of Terms,” n.d. https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/.

PEN America, Online Harassment Field Manual. “Documenting Online Harassment,” n.d. https://onlineharassmentfieldmanual.pen.org/documenting-online-harassment/.

PEN America, Online Harassment Field Manual. “Fight Back/Write Back,” n.d. https://onlineharassmentfieldmanual.pen.org/fight-back-write-back/.

PEN America, Online Harassment Field Manual. “Guidelines for Talking to Employers about Abuse,” n.d. https://onlineharassmentfieldmanual.pen.org/guidelines-for-talking-to-employers-and-professional-contacts/.

PEN America, Online Harassment Field Manual. “Guidelines for Talking to Friends and Allies,” n.d. https://onlineharassmentfieldmanual.pen.org/guidelines-for-talking-to-friends-and-loved-ones/.

PEN America, Online Harassment Field Manual. “Legal Considerations,” n.d. https://onlineharassmentfieldmanual.pen.org/legal-considerations/.

PEN America, Online Harassment Field Manual. “Legal Resources for Writers & Journalists,” n.d. https://onlineharassmentfieldmanual.pen.org/legal-resources-for-writers-and-journalists/.

PEN America, Online Harassment Field Manual. “Protecting from Doxing,” n.d. https://onlineharassmentfieldmanual.pen.org/protecting-information-from-doxing/.

PEN America, Online Harassment Field Manual. “Protecting from Hacking and Impersonation,” n.d. https://onlineharassmentfieldmanual.pen.org/protecting-from-hacking-impersonation/.

PEN America, Online Harassment Field Manual. “Reporting to Law Enforcement,” n.d. https://onlineharassmentfieldmanual.pen.org/reporting-to-law-enforcement/.

PEN America, Online Harassment Field Manual. “Reporting to Platforms,” n.d. https://onlineharassmentfieldmanual.pen.org/reporting-online-harassment-to-platforms/.

PreciseSecurity.com. “Top 10 Countries and Cities by Number of CCTV Cameras,” December 4, 2019. https://www.precisesecurity.com/articles/top-10-countries-by-number-of-cctv-cameras/.

Privacy Rights Clearinghouse. “Is a Website That Has Outdated Information about Me Allowed to Charge Me to Take It Down?,” n.d. https://privacyrights.org/resources/website-has-outdated-information-about-me-allowed-charge-me-take-it-down.

Protection Against Stalking. “What to Do! | Protection Against Stalking,” n.d. https://www.protectionagainststalking.org/what-to-do/.

Rogers, Katie. “Leslie Jones, Star of ‘Ghostbusters,’ Becomes a Target of Online Trolls.” The New York Times, July 19, 2016, sec. Movies. https://www.nytimes.com/2016/07/20/movies/leslie-jones-star-of-ghostbusters-becomes-a-target-of-online-trolls.html.

Rosenblatt, Kalhan. “New Jersey Family to Sue School District after 12-Year-Old Daughter’s Suicide.” NBC News, August 1, 2017. https://www.nbcnews.com/news/us-news/new-jersey-family-sue-school-district-after-12-year-old-n788506.

Sample, Ian. “What Are Deepfakes – and How Can You Spot Them?” The Guardian, January 13, 2020, sec. News. https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them.

Sarkeesian, Anita. “Anita Sarkeesian’s Guide to Internetting While Female.” Marie Claire, February 20, 2015. https://www.marieclaire.com/culture/news/a13403/online-harassment-terms-fight-back/.

Satter, Raphael, Jeff Donn, and Nataliya Vasilyeva. “Russian Hackers Fancy Bear Targeted Hundreds of Journalists.” Associated Press, December 22, 2017. https://apnews.com/article/c3b26c647e794073b7626befa146caad.

Schwartz, Bennett Cyphers and Adam. “Ban Online Behavioral Advertising.” Electronic Frontier Foundation, March 21, 2022. https://www.eff.org/deeplinks/2022/03/ban-online-behavioral-advertising.

Seltzer, Sarah. “Beyond Mansplaining: A New Lexicon of Misogynist Trolling Behaviors.” Flavorwire, March 24, 2015. https://www.flavorwire.com/511063/beyond-mansplaining-a-new-lexicon-of-misogynist-trolling-behaviors.

Siekierska, Alicja. “Tim Hortons App Tracking ‘a Mass Invasion of Canadians’ Privacy’: Watchdog.” Yahoo! Finance, June 1, 2022. https://finance.yahoo.com/news/tim-hortons-app-tracking-a-mass-invasion-of-canadians-privacy-watchdog-190134196.html.

Southern California Defense Blog. “6 Winning Defenses to a Stalking Charge,” August 14, 2013. https://www.southerncaliforniadefenseblog.com/2013/08/6_defenses_to_stalking_charge.html.

Stalking Risk Profile. “General Advice for Victims,” n.d. https://www.stalkingriskprofile.com/victim-support/general-advice-for-victims.

StatCounter GlobalStats. “Desktop Browser Market Share Worldwide,” n.d. https://gs.statcounter.com/browser-market-share/desktop/worldwide.

Talbot, Margaret. “The Attorney Fighting Revenge Porn.” The New Yorker, November 28, 2016. https://www.newyorker.com/magazine/2016/12/05/the-attorney-fighting-revenge-porn.

The Guardian. “Amazon’s Ring Is the Largest Civilian Surveillance Network the US Has Ever Seen,” May 18, 2021, sec. Opinion. https://www.theguardian.com/commentisfree/2021/may/18/amazon-ring-largest-civilian-surveillance-network-us.

The Princess Bride. Act III Communications, Buttercup Films Ltd., The Princess Bride Ltd., 1987.

Totem Project. “Totem Project,” n.d. https://learn.totem-project.org/.

Valenti, Jessica. “Insults and Rape Threats. Writers Shouldn’t Have to Deal with This | Jessica Valenti.” The Guardian, April 14, 2016, sec. Technology. https://www.theguardian.com/commentisfree/2016/apr/14/insults-rape-threats-writers-online-harassment.

Vermont Secretary of State: Corporations Division. “Data Broker Search,” n.d. https://bizfilings.vermont.gov/online/DatabrokerInquire/DataBrokerSearch.

Victim Connect Resource Center. “Victim Connect Resource Center - Confidential Referrals for Crime Victims,” n.d. https://victimconnect.org/.

West, Lindy. “What Happened When I Confronted My Cruellest Troll.” The Guardian, February 2, 2015, sec. Society. http://www.theguardian.com/society/2015/feb/02/what-happened-confronted-cruellest-troll-lindy-west.

Whitman, Ryan. “Judge: Police Can’t Force You to Unlock Phone With Fingerprint or Face ID.” ExtremeTech (blog), January 15, 2019. https://www.extremetech.com/mobile/283795-judge-police-cant-force-you-to-unlock-phone-with-fingerprint-or-face-id.

Women’s Media Center. “Online Abuse 101,” n.d. https://womensmediacenter.com/speech-project/online-abuse-101.

Woolley, Samuel C., and Philip N. Howard. “Computational Propaganda Worldwide: Executive Summary.” Computational Propaganda Research Project. University of Oxford, Oxford Internet Institute, n.d.

Zeltser, Lenny. “Network DDoS Incident Response Cheat Sheet.” Lenny Zeltser (blog), September 23, 2016. https://zeltser.com/ddos-incident-cheat-sheet/.

Zhang, Xiaolu, Ibrahim Baggili, and Frank Breitinger. “Breaking into the Vault: Privacy, Security and Forensic Analysis of Android Vault Applications.” Computers & Security 70 (September 2017): 516–31. https://www.sciencedirect.com/science/article/pii/S0167404817301529.

# Index

For every working professional, it's important to balance the demands of their income-generating, outward-facing, social persona against their irreplaceable, valuable private life.

Whether you are a rising associate or a C-level executive, separating and insulating your personal life from your public one is critically important so you can protect yourself, your loved ones, and the many non-work aspects of your life that you hold dear and precious. After all, what's the point of working so hard on our careers if we allow the personal aspects of our life to be harmed, violated, or exploited?

Personal Privacy for Professionals provides actionable strategies and practical tactics you can employ to protect your private life immediately.

The authors have helped numerous professionals who have been harassed, stalked, or threatened by disgruntled employees, internet trolls, online abusers, and anonymous threat actors. While those threat actors may have been triggered due to the victim's public or professional face, the abusers inevitably target or threaten the victim's private life because the abusers know that is where victims are most vulnerable and have the most to lose. In today's world, unfortunately, any working professional (and even retired professionals for that matter) may be vulnerable for the same type of unwelcome attention and abuse. What's even worse, many times the vitriol or anger that gets directed at a victim may not even have a triggering reason for occurring in the first place -- sometimes victims are targeted at random.

Regardless of why, how, or when it occurs, we do know for a fact that victims never expect it to happen and are often blindsided when their privacy does get violated.

We want to prevent that from happening to you.

Personal Privacy for Professionals covers both your physical world privacy and online privacy with clear, easy-to-understand directions that you can begin employing immediately. We intentionally avoid jargon or lengthy technical discussions and instead get to the guts of the matters fast.

PS PRINCETON STUDIOS