Privacy Code 2.0:

How to Protect Your Privacy From the Next Attack

BANYAN HILL

Privacy Code 2.0

How to Protect Your Privacy From the Next Attack

By Ted Bauman
Editor, *The Bauman Letter*

IN the late 1980s, when I was a student at the University of Cape Town, the South African system of apartheid was in its death throes.

It was hard to tell that at the time, of course: The police state was everywhere — on your phone line, in your mail, in your workplace, watching your movements.

They even made it into my bedroom — the ultimate private space.

Like most South African university students, I was active in the anti-apartheid movement. I attended rallies, got tear-gassed and participated in strategy meetings. I wrote political pamphlets that were posted anonymously around the university and the neighborhoods where students gathered at night to drink and watch live music. I taught undergraduate courses where my views — liberty and equal rights for all, regardless of color — were in plain view.

But none of that brought the security police to my door. They came because of a private and personal issue: My girlfriend wasn't white.

Under the Group Areas Act, it was a crime for a "nonwhite" person to live in an area reserved for "white" people. My girlfriend was classified "colored" (mixed race) under apartheid law. Both postgraduate students, we lived in a flat in the City Bowl section of Cape Town.

By the late 1980s, the police had much bigger fish to fry than Group Areas violations. Nevertheless, somehow or other I had come to their attention. So they came to my door one fine spring day and demanded to search my home. (No search warrants were needed in those days.)

After going through my library, writing down the titles of political tracts and photographing political posters on the walls, the police moved on to our bedroom. Using a riding crop — a sort of "swagger stick" carried by police colonels — they rifled through our clothing drawers.

Their leader, a typical Afrikaner with a big belly and a thick snorr (moustache), lifted one of my girlfriend's undies and slowly looked up at me. He said nothing, merely putting the clothing back in the drawer and closing it slowly.

As they prepared to leave, the squad leader turned back, and said, in the classic affectation of a TV police detective, "One more thing."

I knew then I was done for.

"We know all about you, Mr. Bauman. We know you spoke to X yesterday for 20 minutes on the phone, and what it was about. We know about your pamphlets. We know what you're teaching our kids at that communist shithole of a university up on Devil's Peak. We even know what rubbish you're writing to your family back in the States. We can deal with that. But this arrangement of yours" — he gestured around the flat — "is a step too far. Best see to it. Good day."

I can't say I was stunned, since I had it coming, as it were, but I was deeply shaken. I assumed I would be deported forthwith.

I wasn't. Instead, life went on, albeit under a cloud of uncertainty that changed everything. I presumed everything I did and said was monitored and recorded somewhere. Since I wanted to continue living in South Africa, which had become my home, I had little choice but to withdraw from open political activity, shut my mouth and hunker down like Winston Smith from George Orwell's 1984.

My experience all those years ago turned me into a staunch defender of civil liberties and privacy. It also prompted me to learn many techniques to conceal my online identity and to become "invisible" to the prying eyes and ears of government and others. And now I'm going to share these techniques with you, so you too can appear to be "off the grid" … while still being on it.

Learn From the Pros

I've always been fascinated by celebrities such as the rubber-faced actor Eddie Murphy.

That's not because of their talents — although Murphy certainly is talented — but because of their ability to secure the details of their private lives from public scrutiny. Murphy and a handful of other A-list celebrities are renowned for preventing knowledge of their private affairs from leaking beyond their own inner circles.

But what about you? Are you able to keep your life as private as you'd like?

Consider who's after your information. We know about the National Security Agency, FBI and other government agencies that routinely abuse our privacy rights. For example, no one has Fourth Amendment privacy rights when crossing the U.S. border. Border agents can copy all of the files off of your computer or phone. This is also true in Canada and in other countries around the world.

But there are plenty of more immediate threats relevant to you and your affairs.

Private companies take your details and store them on servers that can be hacked. Websites you visit are tracking your every move on the internet and passing on that information for profit to Lord knows who. Lawyers, business competitors, estranged family members — and blackmailers — would just love to get their hands on information they could use against you.

If celebrities can protect their personal information, so can you … but first, we've got to be clear about what we mean by this thing called "privacy."

What Is Privacy?

Privacy isn't really a "thing" — *it's a state of being*, supported by a range of actions and processes. It's something you do, not something you are. And even if you believe you're technically entitled to privacy by law, the Constitution or natural rights, you're not going to have it unless you take action.

The practical definition of privacy varies from person to person. It depends on the specific information you want to protect. It also depends on the nature and location of that information. Some people are perfectly happy to have the rest of the world be aware of their existence and of certain basic facts about them … but nothing more. Other people seek complete anonymity.

Besides being specific to each person, the concept of privacy has two facets:

1. **The condition of being free from being *observed or disturbed* by other people — the "right to be let alone."** That's what Supreme Court Justice Louis Brandeis called it in a paper for the *Harvard Law Review* back in 1890. It's the type of privacy most people instinctively think of when they hear the word. It conjures up images of home and hearth — your "castle."
2. **The right to *control access to personal information*,** much of which exists outside your own personal castle — on the internet, or in the hands of banks or other businesses, for example. "Information privacy," as I will call it, involves four elements. First, it's about information. It emphasizes knowledge about you, rather than, say, physical proximity to you. Second, it refers to personal information — your identity,

thoughts, aspirations, passions, habits, idiosyncrasies or indiscretions — as well as your assets and finances. Third, it's about control. It's not how much or how little is known about you, but whether you can choose which information is revealed and to whom. Finally, privacy is a right.

At its core, privacy is a state of being that allows you and only you to choose what other people can observe or know about you. In that sense, privacy is about *control* … and thus at the very heart of personal sovereignty and individual liberty.

But privacy is also about *dignity.* Without privacy, we are like bees in a hive or ants in their nest. Our individual personality, moral character, personal autonomy and independence vanish, and our existence is reduced to an element of a larger group, subject to its priorities. This is why totalitarian collectivist societies such as Nazi Germany and the Soviet Union focused so much on surveillance — it simultaneously eliminated individual choice and control and abolished personal dignity in favor of a supposed dignity deriving from the people and the party that claimed to represent them.

Privacy, Security and the Sovereign Life

If privacy is a state of control and choice over information about us, security is the range of techniques we deploy to acquire and preserve that state.

Because there are so many different types of privacy and information, security techniques vary widely, from the mundane to the complex.

To understand this, I find it helpful to break privacy into three discrete elements. They overlap, but they're not the same, and the strategies you adopt to secure them are often quite different.

1. **Anonymity:** This is the state of being nonidentifiable, unreachable or untraceable. Some people value anonymity for its own sake, but more commonly, it's seen as a way of realizing privacy. Most people seek anonymity in some contexts but not others.
2. **Security of information:** Most of the information about us that we wish to protect "sits" somewhere passively most of the time. Your computer's hard drive, your file at your doctor's office, your web-surfing history and a merchant's record of your purchases — these are examples of information that must be protected but generally aren't in motion.
3. **Security of communication:** Related to security of information but distinct from this is security of communication. The techniques we use to secure static information (a safe, locked filing cabinet, disk encryption, passwords, etc.) are not the same as what we use when transmitting that information from one place to another. When private information is in transit, we need a different set of techniques to secure it.

In what follows, I'm going to be focusing on *information and communication security* — those aspects of privacy that correspond to "the right to control access to personal information," the second aspect of privacy I identified above.

Assessing Your Need for Privacy: Threat Modeling

The search for privacy starts with a *realistic* assessment of your privacy risk. Before you decide what tools you need to use to protect your privacy, you must understand the threats you face as best you can. That involves identifying what you need to protect and *from whom* you need to protect it.

After all, only the genuinely paranoid will want to adopt every single privacy-protection technique available at all times. Most of us will want to "model" the realistic threats to our privacy and balance those risks against the potential rewards of addressing them.

When modeling the threats to your privacy, there are five main questions to ask yourself:

1. **What do you want to protect?**

   Think of information about you as an asset. An asset is something you value and want to protect — for example, your emails, contact lists, instant messages, phone calls and computer files. Your devices — PC and phone — are also assets. Just as you would do an inventory of your personal assets for an insurance policy, you want an inventory of your privacy assets for your privacy strategy.

   Step 1: Write down a list of sensitive information about youself, where it's kept, who has access to it and what currently stops others from accessing it.

2. **From whom do you want to protect it?**

   An "adversary" is any person or entity that could pose a threat to your privacy assets. Examples include your business partners, government, hackers and fraudsters. Adversaries' motives differ widely, as do their methods of attack.

   For example, if you have significant personal wealth, you might want to make it difficult for potential litigants and their lawyers to find out about it. Or you might be in sensitive negotiations with a potential business partner and seek to prevent it becoming a bargaining chip. Or you might simply not want the government reading your emails.

   Step 2: Make a realistic list of who might want to gain access to your private information and what they might want to do with it.

3. **How likely is it that you will need to protect it?**

   It's important to distinguish between threats and risks. A threat is a bad thing that can happen, but risk is the *likelihood* that it will.

   For instance, there is always a threat that floods might damage your home. But the risk of this actually happening is far greater in New Orleans than in Denver. You can apply the same logic to your privacy assets.

   For example, your mobile phone provider has access to all of your phone records, and could conceivably use that data against you. While your mobile phone provider has the capability to access your data, the risk of them doing so for any purpose that could harm you is low. On the other hand, if you know you are the target of an investigation, either by legal authorities or a litigant, you might well be concerned that they would try to obtain your phone records with a court warrant. That would dramatically increase the risk of your mobile provider's data threat.

   Similarly, a hacker can access your unencrypted laptop or smartphone communications on an open Wi-Fi network. If you're texting your wife to see what to pick up for dinner, that might not matter. But if you're emailing your attorney about a legal matter it might — a lot.

   Step 3: Survey your personal affairs to see where you are at the greatest risk of a privacy breach and prioritize securing those assets.

4. **How bad are the consequences if you fail?**

   Threats and risks are really defined by their potential consequences. In the examples above, I illustrated a change in risk by reference to a chance of potential consequences. When you identify threats and their likelihood of happening, you also want to identify the costs to you if they happen.

   Step 4: Rank the risks to your privacy assets that you identified in Step 3 in order of most to least consequential.

5. **How much trouble are you willing to go through to prevent those consequences?**

   Assessing threat and risk is a personal and subjective process. Some people find certain threats unacceptable no matter what the risk, because the mere presence of the threat at any likelihood is not worth the cost. They are willing to do, more or less, whatever is necessary to prevent it. In other cases, people disregard risks because they don't view the threat as a costly one … or because it's essentially a matter of chance, there isn't much they can do about it.

Step 5: Keeping the rank you developed in Step 4 as a reference, group your privacy risks into three buckets: Essential, Optional and Nonessential/Chance.

With the ranking and grouping you've developed, you can see immediately which threats you should address, and in what order: Start with the most consequential privacy threats in the Essential bucket and work your way down. Even if there are consequential threats in the other buckets, you've decided that they can wait — usually because there are limits to what you can do about them.

Information Privacy Essentials

There are two critical elements of a personal information privacy strategy that rarely get a mention in most treatments: the importance of trust and the close link between information privacy and information security.

Who Can You Trust?

Earlier, I distinguished between "security of information" and "security of communication." The former is static information, such as your computer's hard drive, your medical files, internet history and transaction records held by entities with which you've done business, like banks. The latter is any information in transit, such as emails, telephone calls or real-time web browsing activity.

One thing that's immediately apparent is that protecting your information privacy involves other people and organizations. Your medical and banking records are held by others, and every email or phone call has someone on the other end. How can you control what they do with your information?

When it comes to communications, it's possible to use technologies that prevent the recipients of your emails, texts or phone calls from sharing them easily. But even if you do that, the information is still stored in their heads. Similarly, you can insist on doing business with firms that use the highest-quality information security protocols, but if they decide to hand over your information to someone else, you're toast.

That's why, before I talk about any fancy technological solutions, I want to emphasize how important it is to be selective in your business and personal relationships. Controlling your privacy risks starts with choosing trustworthy partners. There isn't any technology that can prevent an unscrupulous or weak-willed financial adviser from handing over your files. Similarly, even a self-destructing, unprintable email is worthless if the recipient has an adversary reading it over their shoulder.

Of course, the threat-modelling technique I outlined above is critical here. I don't particularly trust Amazon.com, but on the other hand, it doesn't have any information that could really hurt me — as long as I take certain basic precautions. Similarly, my everyday retail bank isn't a big privacy worry (other than credit card transaction records — see below), unless I recklessly conduct sensitive transactions through those accounts.

But if I had a psychiatrist, an independent asset manager in Switzerland, or if I was a collector of rare stamps or coins — in those cases, due diligence and my partners' reputation and probity would be my first line of defense against privacy threats.

The Security Paradox: Digital Is Safer

I recommend you turn your sensitive personal information into digital form. That's because in addition to privacy, I also want it to be secure from loss or destruction.

A lot of what's important to us is on paper — passports, birth certificates and so on. So are personal mementos such as photographs or home movies. What if that paper is destroyed or stolen? Any document can be duplicated, but there are physical limits to storing such copies. You can keep some important things away from your home, like in a safe-deposit box, but that's not practical for most important life documents. Making copies of insurance contracts, for example, and storing them elsewhere in your home would be useless if it burned down. Making physical copies of photos would be expensive and pointless.

But once you turn these things into digital form by scanning them, you can store them in multiple locations, both on- and off-site, that are instantly available to you. For example, if you lose your passport when you're abroad, many countries will allow you to travel with a digital copy certified by a U.S. consulate — if you have one.

I routinely scan all important documents — such as passports, birth certificates, receipts, warranties and so on — to Adobe Acrobat (PDF) files and store them on my home computer. I back up that computer to a special hard drive contained in a small fire- and waterproof safe that has a network connection built into its side. Every day my computer automatically backs up my data to that drive, which is bolted to the foundation of my house and accessible via a hidden door in the basement floor. Even if a gas leak blew the place up or a tornado roared through, I'd still have digital copies of my records.

And because it's so small and hidden away, that safe would be overlooked by any thief outside my intimate circle. But even if a thief found it and managed to pry it loose, I'd still be fine.

That's because I also store my important records in "the cloud," using an automatic online backup system on secure servers in Switzerland. It costs me very little … about $5 a month. I can access those servers from anywhere in the world.

Digital records can't replace all physical documents, of course. But having digital copies of the key ones makes it infinitely easer to replace them if that becomes necessary.

Pause for a moment and consider what personal information you have in your home that's important to you, where it is and what threats it might face.

For example, some of your photographs and home movies are probably in a shoebox in a closet, where they are vulnerable to fire, flood and theft. You probably have digital copies that could be lost due to computer malfunction, theft or hacking.

Your life documents, such as passports, birth certificates, marriage documents, educational records and so, on are probably in a safe or filing cabinet. Like your photos, they're vulnerable to destruction or theft. You probably have a mix of business and employment records, tax files, insurance documents, an asset inventory, wills and other estate records, and warranties, receipts and manuals in both physical and digital form.

The fact is that any personal information in physical form is vulnerable to all sorts of risks. Few people have big fire- and waterproof filing cabinets and safes for their papers. While digital information is less vulnerable than physical papers, it faces its own threats ... unless you encrypt it. That's the bedrock of all digital information privacy and the one technological aspect of privacy that's important to understand clearly.

Encryption: Information *Only You* Can Use

In the movies, an industrious gang of burglars usually gets what's in the safe. We might even cheer them on as likeable underdogs.

But imagine a scenario in which the purloined safe's contents remained useless to them, even after they had cut it open and held it in their hands. They could see it and touch it, and knew what it was worth, but they couldn't do anything with it. The rightful owners of the property had taken steps to render it useless to anyone but them.

Movie safes hold gold, jewels, bearer bonds or other valuables. But there's another form of wealth that's just as important … and which can be protected in a way that leaves even the cleverest thief high and dry: personal information.

As I explained above, I routinely digitize my important personal documents and artifacts and store them in a "digital safe" as well as on a secure server in Switzerland. You may think I'm taking great risks doing this. It's bad enough that I'm turning my passports and other important papers into digital form where they could be hacked, but I'm also storing them on a server I've never seen, in a foreign country, run by people I've never met. Right?

Not at all. That's because everything on my computer and in the cloud is *encrypted.*

NSA whistleblower Edward Snowden — who knows a thing or two about encryption — maintains that "Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on." And if the directors of the FBI and the NSA don't like encryption — *they hate it* — it must be worth it.

Encryption is used at many different stages in the handling of digital information. The two most important are when information is in *storage* and in *transit* — what I call *static* and *dynamic* information environments. Encryption is the bedrock of information security.

How Encryption Works for You

To protect my papers, photos and other information, I used a combination of *full-disk encryption* and *file encryption*, which I'll explain below in more detail. They both work by using special software to scramble digital information into seemingly random sequences of letters, digits and symbols. It can be unscrambled only with a special "key," such as a password or passphrase.

As an example, here's how full-disk encryption works — a task that can be completed in under an hour and is essential to every laptop that travels with you. Without disk encryption, if someone gets physical access to your computer — like the several laptops I've had stolen in my travels over the years — they can easily see the content of all your files.

When you switch on your encrypted computer, before your operating system — like Windows or Apple Mac — can boot up, you must first "unlock" your disk by typing in a password or passphrase. This, in turn, unlocks a special encryption key on your disk, which then unlocks everything on the disk for as long as the computer remains on. (This two-step approach lets you change your passphrase without having to re-encrypt your disk, and also makes it possible to have multiple passphrases — for example, if you add a user account for your spouse.)

Once your computer is on and you've entered your passphrase, your disk is completely transparent to anyone using it and to the applications on your computer. Files open and close as they normally would, and programs work just as they would on an unencrypted machine. You won't notice any performance impact.

By contrast, your Windows or Mac OS passwords don't protect you at all. An adversary can simply boot your computer to another operating system from a USB stick, bypassing your password, to look at your files. Or they can remove your hard disk and put it in a different computer.

But with strong disk encryption, they won't be able to read a thing on your computer's drives — *ever.*

Note that disk encryption is only useful against attackers who have physical access to your computer. It's still possible for your computer to be hacked and for individual files to be stolen when you've unlocked it and connected it to the internet. Disk encryption also doesn't protect your activity on the internet itself.

That's why I distinguish between static and dynamic information environments — you need a different set of tools for the latter, as I will show.

The Trick to Creating the Right Password

Passwords and passphrases are absolutely critical to all of your information security efforts. They may seem anodyne, but they are the single most important thing protecting your encrypted data. It's important to understand how they work and how to develop a good one.

Passwords are assessed in terms of "entropy." Entropy is measured in bits, and determines how many guesses it would take to crack the password.

For instance, a single six-digit password in 32-bit encryption would take 4,267,967,296 guesses to crack. It would take approximately a month and a half for a supercomputer to try all those guesses. That's what the NSA and Britain's Government Communications Headquarters (GCHQ) do for a living.

But a seven-word 128-bit passphrase like "waltzed assemble maverick tonsil subsumes gunner submarine" would require 165,874,258,366,850,931,470,183,446,872,064 guesses. At 1 trillion guesses per second, it would take 27 million years for supercomputers to crack this.

That's why passphrases are the preferred approach to true digital security these days — not individual passwords. For the really important things, you want to use a passphrase.

Here's how to generate totally random passphrases using dice and a word list. You roll a six-sided die five times, and write down the numbers that come up. If you roll the number two, then four, then four again, then six, then three, then look up 24463 in the Diceware word list (http://World.STD.com/~reinhold/dicewarewordlist.pdf), you'll find the word "epic." That would be the first word in your passphrase. Repeat until you have a seven-word passphrase … one that the NSA and GCHQ couldn't break in 27 million years.

Protecting Passwords … From Yourself

Of course, with strong disk encryption, you must be extremely careful. If you forget your passphrase, you'll be locked out of your own computer, losing your data forever. Nobody can help you. That's the point of disk encryption, after all.

For that reason, memorization and/or secure storage of your passphrase is critical. My critical passwords, for example, are stored in two separate ways.

- The master encryption passport is printed out, laminated to protect from moisture and stored in the special information safe I described earlier. (Why not in a safe-deposit box? Because it would be vulnerable to court orders served on my bank.)
- I've given a copy of the master password to that encrypted file to someone I trust … for you, it could be a friend, attorney or relative.

Tools for Total Personal Information Security

Several times so far I've distinguished between static and dynamic information security. Think of the distinction as akin to techniques for protecting portable physical assets. Static security is your digital safe. Dynamic security is your digital armored car. In addition, there's the question of protecting the information that others have about you. Let's consider tools that you can use to achieve each of the goals in turn.

Before we do, it's important to understand that I prefer open-source security software for a reason. "Open-source" simply means that it is developed and distributed for free by committed privacy advocates, rather than by for-profit firms.

That may seem paradoxical — after all, the market is supposed to be a solution to everything, right? Not always. The problem is that encryption software from commercial software companies may have government-friendly "back doors" built in. Such proprietary "closed-source" software is easier for adversaries to manipulate than open-source software, since nobody can see what's in it, or modify it.

By contrast, open-source software is free to share and modify, and can be opened up and analyzed by anyone. That way any bugs or malicious privacy-defeating "backdoors" are impossible to hide. Vendors who use open-source software for security applications focus on developing user-friendly interfaces for this underlying free code.

The software I'm going to recommend is ALL based on open-source encryption and other protocols that security researchers are constantly trying to break — just to make sure they are safe. The NSA and other potential adversaries can't install secret backdoors in open-source encryption software, since it is more likely to be discovered given the many people constantly working on it.

Static Information Environments

Static information is usually contained on your computer, laptop or phone. There are two basic ways to encrypt this information.

Full-disk encryption protects your entire computer's or phone's data in case it is stolen or breached. It works on laptops, PCs and smartphones. The goal of disk encryption is to prevent someone who gains access to your computer — such as a lost or stolen laptop or phone — from reading the files stored on it. Ever. For full-disk encryption, I recommend DiskCryptor. It uses 256-bit encryption, managed by the Electronic Frontier Foundation, one of the best outfits around dedicated to digital security. It's easy to set up and use.

File encryption does the same thing, but on a file-by-file basis. Even if an encrypted computer is hacked, individually encrypted files are invulnerable. The goal is to lock down your most sensitive files — whether they're photos, financial documents, personal backups or anything else — and keep them locked down so only you have the key. Here are some that I have tested and recommend (in no particular order):

- GNU Privacy Guard is an open-source implementation of gold-standard encryption tool Pretty Good Privacy (PGP). Most people choose GPGTools, an all-in-one solution that offers file, email and disk encryption for Windows and Mac. It uses 256-bit AES encryption standard, the most common.
- VeraCrypt is a successor to a long-popular program called TrueCrypt, which ceased development in 2014. It's free, with versions available for Windows, Mac and Linux. VeraCrypt supports the 256-bit AES standard and allows the creation of hidden, encrypted "disk volumes." It is under constant development with regular security updates. In addition to its security precautions, VeraCrypt supports plausible deniability by allowing a single "hidden volume" to be created within another volume. In other words, it has the ability to create and run a hidden encrypted operating system whose existence can be denied.
- AxCrypt is a free open-source encryption tool that integrates nicely with Windows. You can right-click a file to encrypt it or configure "timed," executable encryptions, so the file is locked down for a specific period of time and will self-decrypt later, or when its intended recipient gets it. Files with AxCrypt can be decrypted on demand or kept decrypted while they're in use, and then automatically re-encrypted when they're modified or closed. It's fast, and allows you to select an entire folder or just a large group of files and encrypt them all with a single click. It can also secure files on file-sharing services such Dropbox or Google Drive. AxCrypt supports 128-bit AES and AES-256 encryption standards.
- 7-Zip is actually a file archive utility. As well as compressing and organizing files for easy storage or sending over the internet, it's also a strong file encryption tool, capable of turning individual files or entire directories into encrypted volumes. It's completely free, even for commercial use, and supports 256-bit AES encryption. Compressed and encrypted archives are easily portable and secure, and can be encrypted with passwords and turned into executables that will self-decrypt when they reach their intended recipient. 7-Zip also integrates with the shell of the operating system you're using, making it usually a click away from use.
- AES Crypt is as simple as it comes. It places an option in the Windows Explorer right-click menu, which lets you encrypt the file with a password. AES Crypt will then give you a 256-bit AES encryption version of the file, which can only be opened by someone with the password. You can then email it out, put it on the web for someone to download and so on, in complete safety. It's the perfect tool if you have sensitive information and you want to back up the data at a bank, in a cloud-based storage service and any place where sensitive files might be accessible by someone else.

What about your cellphone? It's a storage device too. Typically, cellphones do not contain files, but rather links to files stored in the "cloud." For this reason, smartphone encryption is generally based on encryption of the entire device rather than its storage "drive" or individual files. For example, all Apple devices from iPhone 6 onward are 256-bit encrypted when you choose to use a password to open them. Everything on the phone — contacts, emails, texts, photos and so on — is only accessible via the password you set for it. Even Apple cannot read it. The same goes for most Android phones, which use Google software.

Dynamic Information Environments

Now that we've considered static information encryption techniques, let's look at ways to protect your dynamic information environment — your communications.

YOUR CELLPHONE/SMARTPHONE

Let's start with the gadget many of us use more than any other: the cellphone. Your approach to security and privacy here will depend on what you want and need to use your phone for.

The first thing to understand is that there are two ways to make phone calls these days. One is via your cell service provider's system. This is completely insecure and can be tapped and hacked by government or private adversaries with ease. You should assume that all your cell calls are compromised.

The other way to make a call is through the Voice over Internet Protocol (VOIP). This is how web-based communications services like Skype work. VOIP converts the audio of your call to a data format that can be sent over the internet. You can make VOIP calls using your cell provider's data bundle or by connecting to wireless.

VOIP makes encryption possible. For example, the Swiss company Silent Circle offers encrypted calling and text plans, as well as data security for when you use your smartphone for email and web browsing. When a Silent Circle subscriber makes a phone call, sends a text or video chats with another Silent Circle member, that VOIP or text transmission is secured and encrypted end-to-end. You can use Silent Circle from an iPhone, Android device, iPad, or even from a Windows or Apple computer.

Silent Circle is interested only in data security and privacy — that's its business model. In fact, its company motto is: Nothing seen. Nothing heard. Nothing disclosed. If it fails, it's finished. The company owns, controls and even custom-builds its own Swiss-based servers, and employs NSA-level security measures to prevent intrusion. It has built its own backbone for its encrypted communications service, and unlike most telecom companies, it doesn't share its dedicated network with third parties.

Silent Circle is best paired with a Blackphone, a self-described "anti-NSA" phone. It looks like a standard Android phone but is preconfigured for privacy with simple tools that anyone can use, and it won't allow you to install vulnerable third-party apps. It offers a level of security and data you certainly won't get with anything else … and it's practically unhackable.

But you can also use Silent Circle-level technology with an Apple iPhone. (Because its operating system is tightly controlled by Apple, and not open source, Apple iPhones are invulnerable to the most common forms of hacking.) To do this, download and sign up for Signal, a secure call and messaging app that uses the same VOIP encryption technology as Silent Circle. I use it and swear by it.

YOUR EMAIL

Email is an important and challenging electronic privacy issue. It's the tool we use most often, and critical for sensitive but complicated transactions such as banking and investing. As with all encryption, email encryption scrambles the contents of your messages. They can be unscrambled only with an "encryption key" that you set and share with your trusted contacts.

There have been a lot of developments since I started working on privacy and encryption a few years ago, driven mainly by the bombshell revelations of Edward Snowden and WikiLeaks. For example, Google and

Yahoo!, providers of free email services to millions, promised in 2014 to work on encrypting all emails sent using their services. But they have yet to roll it out and once those emails are on Google or Yahoo! servers, they are unencrypted — after all, these companies make money by mining their contents for your "preferences." They will never give you full email security.

But the second big development is the emergence of companies and organizations that provide secure email services as their main business. There are a half-dozen such initiatives out right now, but the one I recommend — and which is free — is ProtonMail. I personally use ProtonMail because, being a Swiss company, its servers are based in a jurisdiction that really values personal privacy.

When you send a ProtonMail email, you create a password that the person on the other end has to enter to unencrypt it. You can also set a timer that will "self-destruct" the email after a given period.

The great advantage of ProtonMail is that all encryption takes place on your computer and the receiver's computer. Neither your messages nor your encryption passwords are stored on ProtonMail's servers, so there's no way for the government to get their hands on them, even under the remote possibility of a Swiss court order against ProtonMail. That makes it far safer than services that store your encryption key on servers.

There were two temporary drawbacks to ProtonMail when it was launched in May 2014 that have since been resolved. First, demand for ProtonMail was so high that there weren't enough available servers in Switzerland to accommodate it. Second, ProtonMail didn't encrypt file attachments. Since then, the company has raised more than enough funds for development and now provides end-to-end encryption to any desktop client that supports IMAP and SMTP, such as Microsoft Outlook, Mozilla Thunderbird and Apple Mail for Windows and Mac OS.

WEB BROWSING

Protecting your internet activity involves things as mundane as using password-protected wireless in your home and office and unplugging your webcam and/or microphone when not using it. But that's just the start. Truly secure web surfing and internet activity is only possible by using a virtual private network (VPN).

A VPN creates an encrypted private network for you across the internet. It enables a computer or network-enabled smartphone to send and receive data across the internet as if they were directly connected ("tunneled") to whatever is on the other end, including ordinary websites you visit.

Within a VPN, all the IP addresses of the computers connected to it are hidden from outsiders, and data sent between them is encrypted. That means that even though the VPN is making use of the public internet, it is completely invisible to those without the right VPN credentials. For example, if you connect to a website using a VPN, your computer's location and other personal data are invisible and anonymous, as is anything you do on that website.

Setting up a VPN on your computer or phone involves installing a piece of software that converts your internet traffic into a password-protected, encrypted form. You use the same browser you normally do, such as Google Chrome or Firefox.

Most people make use of paid services ($5 to $20 per month) that host the VPN for you. In assessing such services, the critical thing to look for is that they do not store usage logs of your internet activity on their own servers — if they do, it can potentially be compromised.

Here are few of the best VPN services for home users:

- NordVPN is my personal choice of VPN. It works on Windows, Mac, iPhone and Android phones with a single account. It is highly customizable, and allows you to shop around for the fastest servers. It's highly ranked for privacy, and it's relatively inexpensive.
- ExpressVPN is one of the most popular and successful VPN providers. Headquartered in the British Virgin Islands, ExpressVPN is a vocal advocate for internet privacy rights. It has a network of servers

across 94 countries with great speeds and easy-to-use clients for many phones and operating systems. ExpressVPN keeps no usage logs.

- IPVanish has servers in 60-plus countries and keeps no logs. It even accepts bitcoin. It's a good low-cost provider, recommended if you want a solution that delivers uncompromised security and speeds, whilst keeping no logs.
- VyprVPN is run by global consortium Golden Frog (based in Switzerland), with 70-plus worldwide server locations. It has simple Windows and Mac clients and Android and Apple apps. Up to three devices can be connected at once, with up to 256-bit OpenVPN encryption. VyprVPN does keep connection logs, but not usage logs. It owns its own networks and data centers, based in Switzerland. It also uses its own protocol called "chameleon," which can completely hide the fact that you're using a VPN — very useful in environments where using a VPN can mark you as suspicious. It also allows you to change your IP address and appear local when traveling to countries that impose internet censorship or in schools and workplaces that impart restrictions. That allows you to bypass blocked websites and content and maintain access to an unrestricted internet.

The next step up is to use the Tor Browser. Tor has its own browser interface that allows most users to use the web entirely anonymously. Tor is similar to a virtual private network but has the advantage of being instantly available once installed — and it's free. Tor is also open source, and operated through distributed computers rather than a central server, which means it can't be hacked or invaded at any central point. Tor has become much easier to use and more secure since the Snowden and WikiLeaks revelations emerged, but it remains a more complex technology than a simple VPN service.

CLOUD STORAGE

SpiderOak is a U.S.-based cloud storage company that offers client-side encryption, which means that it allows you to encrypt data locally. The encryption keys, as well as the password through which the keys are generated, are stored on your device, ensuring that no one, including company employees, can view your data.

Founded in 2007, the service shot to fame after Snowden gave it a thumbs up, praising its "no-knowledge" privacy policy, while warning against "wannabe PRISM partner" Dropbox. The Electronic Frontier Foundation (EFF) has also listed the firm in its annual report of companies that stand by their customers when the government seeks access to user data.

The company later implemented a warrant canary, which means that if it receives a government request for user data along with a gag order, the company can't say anything about it, but it can stop saying everything is OK using a special "status" page.

SpiderOak has also released an open-source software that aims to provide developers a simple way to build secure applications. Dubbed Crypton, the software is essentially a framework that lets applications encrypt information within a web browser before it is sent to a remote server. SpiderOak supports Windows, OS X and Linux, and has mobile apps for iOS and Android.

Tresorit also offers end-to-end encryption, with keys stored locally on users' devices. The Switzerland- based company, which was founded in 2011 by Hungarian programmers Istvan Lam, Szilveszter Szebeni and Gyorgy Szilagyi, officially launched its secure cloud storage service after emerging from its beta in April 2015.

The key selling point of Tresorit is that it relies on what the company calls "one of the strongest encryption algorithms on the market," which makes it possible to store and share data without the company's servers getting access to the content. Tresorit claims unmatched security, and to prove this, the company organized a hackathon in 2013 and 2014, offering $25,000 to anyone who could break its cloud storage encryption. Hackers from some top universities such as Stanford, MIT, Harvard, Princeton and more, participated in the event, but nobody could hack the service. The bounty was later increased to $50,000, but no one was able to break the encryption.

The company later added a DRM feature that provides more control for businesses by extending security to documents once they have been shared and during collaboration. This means that you can now modify or remove access to your encrypted content anytime, even if someone has already synced it to their computer. The feature also gives you access to more granular permissions; you can limit copying, printing, screenshotting and more.

Tresorit supports all major platforms, including Windows, Mac, Android, iOS and BlackBerry.

Third-Party Information Security

We've covered phone calls, texts, emails and web browsing. But what about the data about you that's held by others? There are two things to worry about here:

1. Financial account information such as your credit card details that you "give" to a company (say, Target or Home Depot) is stored on their servers and hacked, causing you financial loss.
2. Private companies amass a dossier of information about you based on your web activities, business dealings and other publicly available information, and use it to "profile" you, either for profit or to target you for fraud. Such databases can also be hacked by others for nefarious purposes.

Addressing the first problem is becoming easier thanks to the emergence of new smartphone payment apps such as Venmo, Square Cash, Zelle, PayPal Mobile and Apple Pay, which I use and recommend — especially when abroad.

They don't actually store your debit/credit card details on your smartphone or on their own servers. Instead, they use an encryption technique called "tokenization." This involves converting your card number into a unique, randomly generated sequence of numbers and/or alphanumeric characters. This "token" is stored in a special part of your smartphone's memory that's impossible to decode — even the phone's manufacturer can't read it. When you make a purchase with a payment app, your card information is tokenized, encrypted and sent to the bank, which decrypts it and authorizes the transaction. The token is never stored by either the merchant or the bank. This avoids exposing your real card information number to theft.

Addressing the second problem is another matter entirely. It is really about behavior and state of mind rather than technology.

Data-based profiling is analogous to an old-fashioned detective story. Sherlock Holmes caught his man by assembling seemingly disconnected facts and teasing from them the identity of the criminal. Modern data-mining firms — which are completely unregulated by any federal laws — do it by assembling digital traces of your online activities to identify you. That's why you may see ads for something for which you recently searched on Google suddenly appearing on web pages you visit.

Thwarting this sort of privacy violation involves two things.

First, reduce the amount of information that you provide, knowingly or unknowingly, when you surf the web.

Second, be selective about what you provide to whom, in order to confuse the database so it can't pinpoint you.

Using a private VPN is a good way to start achieving the first goal. But even without one, there are things you can do. Start by only using Google Chrome or Firefox — never Microsoft Internet Explorer (IE). That's because unlike IE, those browsers are easily customizable. With Chrome or Firefox, you can customize for privacy to your heart's content. For example, on my personal Google Chrome installation, I use the following "extensions," which are all free and can be found on Chrome's web store.

- **AdBlock**, which prevents most tracking cookies, as well as blocking banners, pop-ups, malware and more.
- **Collusion,** which shows, in real time, what information websites silently send and receive to and from other websites that I never directly visit, so I can stop it.

- **HTTPS Everywhere**, which encrypts my web traffic on most sites. This free and open-source browser extension automatically makes websites use a more secure HTTPS connection instead of HTTP.
- **IBA Opt-Out,** which prevents Google and other sites from tracking my browsing habits for advertising purposes.

Combined, these little tweaks make me almost impossible to track. But just to be safe, I also disable almost all the tracking features on Google. I also make sure I log out of Facebook, Google (including Gmail and YouTube), LinkedIn and so on when I'm browsing — if you're logged in, those companies will be able to track most sites you visit for marketing purposes.

To go one step further, you can scrub information about you available online, by using a service such as http://www.Reputation.com to remove personal information from websites that market it. This doesn't work for everything, and in some cases you need to ask to have your personal data removed from a company's database.

Finally, never fill in unnecessary or optional information in online forms. Use made-up information unless it is absolutely necessary to provide accurate information.

Hack Attack!

Thus far in this report, I have addressed techniques you can use to protect your private data whether you're at home or on the go. But that's hardly the only privacy issue we face.

When we think of "private data," we naturally picture things like sensitive documents, bank statements, passwords and other things that are under *our* control. The tools we use to protect those things are designed to prevent other people from getting access to them, i.e., from having them leave our control.

But there's a whole other set of data about you that isn't in your control. That's the information that modern companies acquire about you in the course of your digital — and even nondigital — activity.

Here's a partial list of the types of companies that maintain highly detailed files about you. In most cases, we give this information to them voluntarily, in exchange for a service that we get for free (e.g., Facebook). In other cases, the companies collect information about us from third parties, without our even knowing (e.g., credit bureaus):

- Social media and search companies such as Facebook and Google.
- Online shopping companies such as Amazon and Walmart.
- Credit bureaus such as Experian, TransUnion and Equifax.
- Specialized consumer data companies used by employers, landlords and others.
- Third-party advertising web trackers.
- Banks and other financial institutions.
- Retail stores where you have an account, even if it's not a credit account.
- Rewards programs.
- Hospital groups.
- Insurance companies.

These are just a few of the companies that collect huge amounts of information about you and centralize it on massive servers, where it can be analyzed, manipulated and used to target you for advertising. It can even be sold to third parties for that purpose.

We have no control over this data, even if the companies give us some sort of "opt out" option. That's because even if the companies agree not to use your information in some way, they remain vulnerable to hacking by those who will.

Aggregated data like this is incredibly powerful. Each individual data point is relatively insignificant on its own. But when put together with all the other information about you, it can create a composite image of you that can be used for all sorts of purposes. Those purposes are often highly profitable, which is why data harvesting and mining has become such a huge business.

Since we are not always customers of the companies who collect this data, we don't have much leverage over them. Many companies collect information about us without our even knowing. Often the first time we learn that they have information about us is when there has been a hack, and it has been exposed to the wild.

The hack of the credit bureau Equifax is an excellent case in point. Hackers managed to get into the company's consumer database and rummage around for several months before they were discovered. Information about more than 140 million Americans, including name, date of birth, address and Social Security number, was stolen and leaked. That's essentially all the information someone would need to engage in identity theft or other forms of fraud against you.

In early 2018, media reported that social media giant Facebook had allowed detailed information on 50 million Americans to fall into the hands of a political targeting operation. Facebook didn't exactly just give this information away, but it might as well have. Its internal rules regarding the use and disposition of all the information it has about us turned out to be laughably weak.

And once information like Equifax's data or Facebook's records is out in the open, that's it. There's no way to put the genie back in the bottle.

What can you do to combat this? Here's my basic list:

- Think very carefully about whether it makes sense to get on to a company's database. Once you're on, that's it. Even if you manage to get a company to delete your information, that's no guarantee that it hasn't already been hacked, or that it might be stored in a way that would allow it to be recovered.
- It goes without saying that everyone should have an active credit-monitoring service. This alerts you to any changes to your credit reports, including new account openings. It's not necessary to pay for expensive subscription services anymore. Most of the major credit bureaus offer credit-monitoring services. Third-party websites such as www.Credit.com and www.CreditKarma.com also offer quick notifications of any activity that happens on your credit record. It's true that these companies make money by channeling credit offers to you, but to my mind, it's worth it.
- The next step up from credit monitoring is a credit freeze. That's when you tell a credit bureau not to release any information about you to anybody who's trying to obtain your credit report. For example, if somebody tries to open a credit card account in your name, and you have a credit freeze active, they won't be able to do it. And you'll get a notification that someone tried. The major downside is that you have to remember to unfreeze your credit record before doing any business that would require a credit poll.
- Use two-step authentication for everything. Two-step authentication is basically a process where, in addition to entering a username and password, you also have to enter a one-time code that is sent by email, text or some other means before you're allowed to log into a service. For example, my bank requires me to enter a code that is sent to an email address that I only use for this purpose every time I log on. However, don't use text notifications for two-step authentication. It's ridiculously easy for hackers to commandeer your cellphone number and have texts redirected to themselves. That would allow them to get into your accounts and clean you out.
- Make sure that you use all the notifications that an online company might offer. Deposits, withdrawals, account modifications, changes of name — anything that happens on your account should result in a notification that comes to you, preferably by email. The quicker you learn about something that you didn't do, the quicker you can fix it.
- Set up strict account modification protocols with your financial institutions, especially your retirement accounts. For example, your IRA custodian could set up a special password that you have to give

verbally before they will make any changes to your account, such as your postal address. Unfortunately, it's frighteningly easy for hackers to convince many financial institutions to change things like that, and have checks mailed to them at your cost. Stringent authentication protocols make this much more difficult for a potential fraudster.

Finally, I always tell people to pay attention to the politics around data and privacy. A lot of the vulnerabilities that we face could have been corrected a long time ago were it not for the powerful influence of tech sector lobbying. We would never stand for this kind of vulnerability in other aspects of our lives. But technology has grown so fast and crept up on us so quickly that our collective safeguards haven't caught up. Insist that politicians do something about it!

Doubling Down

Determined adversaries can beat disk encryption. For example, if you were involved in a legal case, and someone stole your laptop, they could get sensitive information. But you can prevent that if you power off your computer completely when you finish working on it, or when you're outside your home with a laptop.

Here's why: Computers have temporary storage called RAM. When your computer is powered on, your software is constantly writing to and deleting from RAM. When you use disk encryption, as soon as you unlock your encrypted disk the encryption key is stored in RAM until you power your computer off. This allows it to encrypt and decrypt files as you use your computer. Laptops have ports that have "direct memory access," or DMA, including FireWire, USB and others. If an attacker has access to your computer and your disk is unlocked — even when it's in sleep mode — someone can plug a malicious device into your computer and read its RAM, including your encryption key.

There are two other hardware-related issues you need to know about:

- If you have something really important to share, use an "air gap." This is a computer that has never been connected to the internet that also has strong file encryption software installed. You can use such a computer to create files (documents, spreadsheets, what have you). When you want to transfer a file, you encrypt the file on the secure "air gap" computer and carry it to your internet-connected computer, using a USB stick. To decrypt something, reverse the process.
- Before you dispose of a computer (or cellphone), get rid of all the personal information it stores. Use a wipe utility program to overwrite the entire hard drive. Then dismantle the machine and smash it to bits with a hammer — especially the hard disks.

Information Sovereignty Can Be Yours

The path to practical sovereignty over one's own life involves exploring new ideas and acquiring new skills. That's because, at its core, privacy is a state of being that allows *you and only you* to choose what other people can know about you. In that sense, privacy is about *control* … and thus at the very heart of personal sovereignty and individual liberty.

With so much of our personal information now in digital form — a form that has major advantages for the long-term protection of your data, as I've argued here — learning privacy skills is essential to becoming sovereign master of your own privacy.

Kind regards,

Ted Bauman
Editor, *The Bauman Letter*

Banyan Hill
P.O. Box 8378
Delray Beach, FL 33482 USA
USA Toll Free Tel.: (866) 584-4096

Email: http://banyanhill.com/contact-us

Website: www.banyanhill.com

LEGAL NOTICE: This work is based on what we've learned as financial journalists. It may contain errors and you should not base investment decisions solely on what you read here. It's your money and your responsibility. Nothing herein should be considered personalized investment advice. Although our employees may answer general customer service questions, they are not licensed to address your particular investment situation. Our track record is based on hypothetical results and may not reflect the same results as actual trades. Likewise, past performance is no guarantee of future returns. Certain investments such as futures, options, and currency trading carry large potential rewards but also large potential risk. Don't trade in these markets with money you can't afford to lose. Banyan Hill Publishing expressly forbids its writers from having a financial interest in their own securities or commodities recommendations to readers. Such recommendations may be traded, however, by other editors, Banyan Hill Publishing, its affiliated entities, employees, and agents, but only after waiting 24 hours after an internet broadcast or 72 hours after a publication only circulated through the mail.