How To Become Untrackable – Part 3

- *As technology has changed our lives, it has also changed crime. Please don't make it easier for criminals that it already is.*
- *Bad guys use aliases, good guys use alternate identities. If you aren't a citizen journalist yet, become one.*
- *Rigorous compartmenting can successfully protect privacy even if you do not stay on top of every little change in technology.*
- *Accounts like Yahoo, Microsoft and Google keep tracking your browsing history even when turned off, which they say is for your own good (to show you the right ads) so log out when you're not using them.*
- *In one way or another, you either give companies data or consent to them stealing it, so stop giving it out.*
- *Next time you move, don't fill out a change of address. Contact companies and contacts and give them a PO Box. Don't send any mail or packages to your residence.*

This is Part 3 of a four-part article on PERSEC/Privacy. Please click here for Part 1, here for Part 2 and here for Part 4.

Where are you on the road to privacy? Maybe you haven't gone far at all and still have a ton of information out there. That's OK. Everyone starts somewhere. Part 3 of this series will help you manage your pattern of life and online footprint.

Manage Your Digital Footprint

Kidnapping for ransom brings in approximately 1.5 billion

dollars per year. Let’s imagine that I am kidnapped for ransom in South America. If the ransom is paid, my captors will probably put a bag over my head and suffocate me to make sure I don’t identify them someday. Since I understand that my chance of survival will drop in to single digits if I comply and let myself be transported, I’m wouldn’t hang around to find out. One technique that kidnappers use to keep guys like me under control is to get my name off my ID (and my address if it’s on my driver’s license and I’m carrying it).

Armed with that knowledge, they can then go to social media websites or even paid search sites to gather more information. They want to locate my home and ultimately my family. Once they do, they’ll follow them around and take photos or get a PI to do it (by paying him and giving him a phony story) which they will use to “prove” to me that they can get to my family. To keep me in line, they’ll describe, in gory detail, how my family will be harmed if I try to escape.

Had I managed my online footprint effectively, compartmented (such as kept my legal name compartmented from my address), and made some changes to household SOP and my own pattern of life, a social media search wouldn’t have likely turned up any useful information. Had I used LLC’s formed in states with laws favorable to privacy to rent or buy vehicles and real estate or used nominees, it would be unlikely that a small group of criminals would be able to find my family, simplifying the problem.

Compartmenting

Rigorous compartmenting can successfully protect privacy even if you do not stay on top of every little change in technology. If you take one thing away from this part of the series, I hope that it’s the need to compartment. Departures from compartmentalization usually occur because it is not convenient and unless you really stay on top of changes and

newly discovered vulnerabilities in the technology you use, they can become your undoing.

- **Alternate Identities** – Your legal name is the name under which you file tax returns and are known to the government. Travelers, soldiers, authors, witnesses and undercover agents have all used alternate names to protect themselves and their families. Aliases are used by criminals. Can you have legitimate alternate ID's? Sure. Next time you move, become a citizen journalist and adopt an alternate name. Then become a writer and adopt an alternate name for that too. But, if you use your legal name on a utility bill, a cell phone, computer, etc., both names would come up at the same address during the same time period, tying the alternate name to the legal one.
- **Electronics** – Effective compartmenting means that you have a separate computer and phone for each identity. Devices can also be compartmented according to the risk associated with activities associated with a given identity. Why expose a device that holds the keys to your kingdom when you could use a device that has little to give away should it be compromised? Never use your legal name on your alternate identity gear and vice versa. You also shouldn't use your alternate identity gear at or near your home, work, school, etc. of your legal identity. Even if you store your alternate ID gear in Faraday bags, so it can't transmit, if your home gets searched and it gets found there, then the alternate ID gear will get tied to your legal ID, compromising it and you. Solution? Cache those burner phones away from home! On the way to pick it up? Either leave your legal ID gear at home, or cache it separately before you pick up your alternate. Why? Compartmenting. If you got nabbed with both, you'd be compromised. Stick sliding covers (Targus is one brand) over cameras and microphones, use Faraday or IT forensics bags and wear gloves or wipe

down your gear with your handkerchief before it goes back in its hidey hole.

- **Internet Connected vs Standalone** – Perhaps the best way to make sure that a computer containing sensitive information doesn't get hacked or infected is to store sensitive information on a standalone computer that you never connect to the internet. With few exceptions, Van Eck phreaking being one, a hacker must have physical access to such a computer. Need to connect to the internet? Network a tablet or notebook computer to your internet connection over copper wire instead of wireless networking. Then unplug the computer and store it someplace secure when not using it to greatly reduce the chances it will be hacked, stolen or infected. If this is too much of an inconvenience, turn your computers off when you are done for the night. Most hacks are attempted at night in the hope that users are sleeping instead of monitoring their computers.
- **LLC's & Nominees** – "The secret to success is to own nothing, but control everything." – Nelson Rockefeller

This is sound advice. Registering vehicles and property in the names of LLC's (in privacy-friendly states) or nominees makes it much more difficult to tie them to any of your identities. Same goes for rental agreements and utilities. It also makes them easier to compartment. J.J. Luna recommends having a couple of LLC's with generic sounding names on hand (he calls them "shelf LLC's") in case you need one in a hurry.

Think Twice Before You Give Out Information

You don't have to look very far or hard to find an article written by someone after quitting Facebook or Twitter. While these writers love to shock readers and reel them in with stories of frightening "social media withdrawal" symptoms,

most such articles eventually come clean in the end and report dramatic improvements in quality of life.

Social media provides a sickening an obscene amount on users and is increasingly the go-to tool for private investigators, bounty hunters, lawyers, thieves, predators, scam artists, hackers, law enforcement, creditors, government and business alike. It is a dream come true for anyone who wants to know all about you. The best part about it is that, one way or another, most of that information is provided by you, the user.

Before you add another app or register for another account, ask yourself if you really need it. Will it make a difference in a year? How about in five or ten years? What are the company's privacy practices? Just because you don't give information over the computer doesn't mean that it won't end up online.

If you're more concerned about hiding from criminals, crazy ex's and enraged motorists than from governments, check out privacy companies. They enable anonymous online purchasing, text messaging and masked email accounts and phone numbers. They also make signing up for new services and managing passwords a snap.

Every year, approximately 20% of Americans move. Those who fill out a form requesting that the USPS permanently forward their mail invite severe consequences. J.J. Luna first made me aware of the fact that if you permanently forward your mail when you move, the address you forward it to goes on the National Change of Address List. The USPS licenses this list to more than 500, who combine it with their own lists and sell updated lists to anyone who will pay. They may keep your address indefinitely since there's little oversight to stop them.

Because the USPS keeps addresses on this list for 4 years and

so many Americans move each year, the NCOA List can include up to 160 million addresses any given time. If you fill out that form, you'll make it virtually impossible to keep your name separate from your new address. You can avoid this by not filing a change of address form. Contact everyone you would like to receive mail from and give them the address for a PO Box. If you want to be untrackable, don't receive any mail or packages at your home whatsoever.

Encryption

Encryption should not be relied upon by itself because of the periodic discovery of vulnerabilities in encryption software. despite vulnerabilities mean that encryption is not 100% effective, various law enforcement agencies have thousands of devices in evidence that they are unable to access. Should your computer or storage device fall into someone else's

hands, effective encryption is a much greater obstacle to accessing the data it contains than just a login screen.

- **Encryption & Decryption Should Occur Locally** – If your data is encrypted on a fileserver instead of the device you are using, your data is vulnerable to interception before it gets encrypted.
- **Encrypt Entire Drives** – You may encrypt the entire drive the data resides on or only those files you wish to protect. Encrypting the entire drive makes it more difficult for a hacker to access your encrypted data than only encrypting the files you consider sensitive. Some IT professionals feel that encrypting an entire drive has a downside since it is harder to retrieve data from an encrypted drive that has experienced data corruption. However, I disagree on the grounds that users should create backups (which must also be encrypted) instead of relying on the retrieval of corrupt data because it is unreliable at best. If you have data that is extremely important, store backups locally and off-site in case the building containing the computer burns down, is flooded or suffers another type of catastrophe.
- **Secure the Original Files** – If a user encrypts a file and just deletes it, the file may still exist on the disk and such files can often be recovered. Therefore, encryption software must encrypt files in place or a secure deletion tool must be used. When a file is encrypted in place, the software overwrites the unencrypted file with the encrypted one. Secure deletion tools overwrite
- **Keep Software Up to Date & Inspect Devices** – Because vulnerabilities are patched in updates, devices must be properly and promptly maintained. Inspect devices to ensure that they are free of malware, viruses and keylogger software. Also inspect all devices and cables for hardware that doesn’t belong. If a hacker has

physical access to your device, even for just a couple of seconds, that's enough time to plug in a keylogger or some other device. A keylogger looks like a USB or PS/2 adapter that plugs in between your device and keyboard and logs every keystroke you make and stores it in memory, including any passwords you type in. Some models include date and time stamps, feature gigabytes of memory and WiFi, typically enabling the hacker to retrieve the data without re-entering the building.

- **Encrypt Email** – Use the following to features to protect e-mail:
    - **Use a Foreign Encrypted Email Provider** – The US government has a history of compelling US companies to cough up whatever they want whenever they want. Most companies won't bat an eyelash before handing over your data and the alphabet soup infiltrate any that do. It is much harder, however, for them to get information out of companies based in other countries, especially those who allow users to pay in cash and remain anonymous.
    - **End-to-End Encryption** – With end-to-end encryption, messages (be they emails, text or voice) are encrypted by the sender, on his or her device, and only the sender and recipient have the information needed to decrypt the message contents. Even the company who owns and maintains the service you send the messages over cannot read what the encrypted messages contain.
    - **Self-destructing Email** – Given enough time, encryption can be broken, but it won't do the folks who have your device much good if your email self-destructed before they could read it.
    - **Authentication** – If you recognize the caller's voice when you receive a phone call from a family member or friend, you know who is on the other end of the line. You are authenticating the

communication by voice. Effective email encryption features mutual authentication, meaning that it verifies that you are who the other person thinks you are and vice versa, preventing man-in-the middle attacks. Otherwise, a hacker could pretend the third party you think you are communicating with. He could also pretend to be you when communicating with the third party. He may simply copy the emails and pass them along or he may edit them. For this reason, whether your group uses radios, encrypted email, notes in dead drops or two soup cans and a string, survival communications must feature authentication.

Employ Effective Password Management

- For passwords to work, you can’t give them out, especially over notoriously insecure means such as most instant messaging apps. Hackers also call targets pretending to be tech support and try to use social engineering techniques to get you to cough up sensitive information, including passwords.
- Passwords must be long and contain special characters.
- Passwords must be changed frequently.
- Do not use the same password for more than one account without modification.
- Passphrases are harder to crack than words.
- Make sure to password-protect WiFi connections.
- Create your own logarithm or set of rules for password creation that are easy to remember because of your life experience and do not share them with anyone.
    - Start with a phrase that is easy for you to remember, but hard for someone else to associate with you. Let’s say I need a Facebook password and I feel like it’s run by a band of criminals, so it

would be easy for me to remember the phrase: “breakingthelaw” associated with that provider.
    - Add some capitalization. Let’s make a rule to capitalize it like a title. The password now becomes: BreakingtheLaw.
    - Replace some of the letters with numbers. In the early days, IT security folks used to use numbers for vowels that looked like their letter counterparts like swapping “1” for “I” or “4” for “A”, but this is now built into cracking software, so make it random. The letter “e” is the most common letter in English, so I can easily remember it and I’ll swap it to the number 6. The password now becomes “Br6kingth6law”.
    - Now I’ll add a combination of special characters at the beginning and end, preceding the phrase with “!” and ending with “?” and it becomes: “!Br6akingth6law?”.
    - Now I’ll add the first letter of the site or service the password is for. We will imagine that the password is for Facebook, so I’ll precede the password with that, making it: “f!Br6akignth6law?”
- Applying a similar set of rules to an easily-remembered passphrase will yield a passphrase that is too complicated to quickly decipher. Make your own rules that *you* can remember and don’t share them.
- If you’re changing passwords frequently and never reusing old passwords like you should be, managing all those passwords can be a daunting task. If you are willing to trade a little security for a chunk of convenience, use a password manager.

Two-factor or Multiple-factor

Authentication

Three factor ID uses three of the following factors and two factor ID uses two:

- **Something you know** – A passphrase or pin.
- **Something you have** – A cellphone that enables you to receive a text message containing a one-time password or a hardware token. A hardware token can be a USB dongle, smart card, key fob or a SIM in your smartphone.
- **Something you are** – Biometrics such as fingerprints and face scans.

While each of these factors are vulnerable by themselves, they present a more serious obstacles when used together.

- Passwords can be guessed or obtained under duress.
- Hardware tokens can be obtained by pickpockets or muggers.
- According to Kevin Mitnick, biometrics can often be fooled by low tech, old school methods such as lifting prints with tape and talcum powder of faking out facial recognition by holding up a high res photo of the user in front of the camera.

Using two or more factors creates enough difficulty that hackers generally move on and look for an easier target.

"The easiest way to get a basic security is to download software to use a VPN"

- THECUSTOMIZEWINDOWS.COM

HOW A VPN WORKS?

CONNECTION

A remote access client connects to a private network from a remote location

ENCAPSULATION

Once a connection is established, data packets are encrypted for security

TUNNELING

Once encapsulated, encrypted data pushed to its end location

CHECK IT OUT & FREE IT UP

As packet data sent on its way, the host or network provider continuously checks the VPN to crosscheck security

Once verified, the encapsulated data is unencapsulated and removed from tunneling protocol

BY : WWW.BESTVPNRATING.COM

Use VPN or Tor to Hide Your IP Address

Running VPN uses an ISP (choose a privacy-centric one) to connect to your VPN provider. A VPN provider establishes an encrypted tunnel between your computer and any of thousands of VPN servers across the globe. This way, your ISP only sees that you are using an encrypted tunnel to the VPN provider and the sites you are connecting to don't see your true location. Choosing a VPN provider based outside the USA in a country with better privacy laws than ours creates obstacles for anyone trying to track who you are connecting to. Just keep in mind that although your ISP can't see your encrypted communications, they can still see the VPN provider you connect to, when, for how long and how much data is sent and received. If you aren't using VPN, they can see a whole lot more.

VPN and Tor both have tradeoffs. VPN is faster and easier. But with VPN, your VPN provider knows your real IP address. VPN wasn't designed for anonymity. Tor was and is somewhat safer. Tor is run by volunteers, is slow and has some compatibility issues.

- **Don't Trust a US VPN Provider** – The US government has a long track record of pressuring US companies to give them whatever they want. In rare instances where these tactics don't succeed, they infiltrate them.
- **Research VPN Providers Thoroughly** – You must be able to trust your VPN provider, so do your homework. What happens when governments subpoena their logs? Read the terms and conditions of service carefully. Make sure that their encryption and VPN protocols are not outdated.
- **Don't Think That a VPN Makes You Anonymous** – VPN was not designed for anonymity, so it must be used in conjunction with other privacy tools, such as privacy-

centric browsers and operating systems.

Just Say No … to Cookies

Cookies are tracking files that are saved to your computer. Don’t accept cookies from anyone you don’t want to be able to track your online behavior, which should ideally be no one. If you do accept cookies, delete them at the end of each session.

Avoid Browser Fingerprinting by Using a Privacy-centric Browser

Browserfingerprinting in another way to tack you based on your browser configuration. When you connect to websites, they can see what browser you are using, it’s configuration and the browser extensions you are running, which gives a lot of options, kind of like DNA or fingerprints are used to find criminals, only its less precise.

Sites like panopticlick can measure the uniqueness of your browser. Running a privacy-centric browser like Epic with the fewest possible extensions makes your browser just like far too many others. If you run something less extreme and arguably more convenient in your legal identity compartment, give Firefox a look, but you’ll need to run extensions like NoScript which block JavaScript, Java and Flash because they can be used to run scripts on your computer that compromise privacy and security.

Log Out of Accounts When They Are Not in Use

It used to be that we only needed to worry about our browsers tracking our browser history, but that is no longer the case. Now some sites log our browsing history to profile us in order to better target us with advertising … at least that’s why

they say they are doing it. To avoid this, log out of Microsoft, Google or Yahoo accounts when not in use.

Root Your Smartphone

Phone providers fill phones with all kinds of balloonware … software built for the express purposes of tracking you and slowing down your device, so you'll need a newer one sooner. When you buy a new device, root it and replace the version of the OS from your provider with a clean installation. Your device will run faster and will be safer OS's from providers often lack privacy and security features.

There is so much more I'd like to include in this part, but alas, this is an article, not a book. While this part should get you started, I hope that you continue the process of learning how to protect your privacy.

Here are Part 1, Part 2 and Part 4