

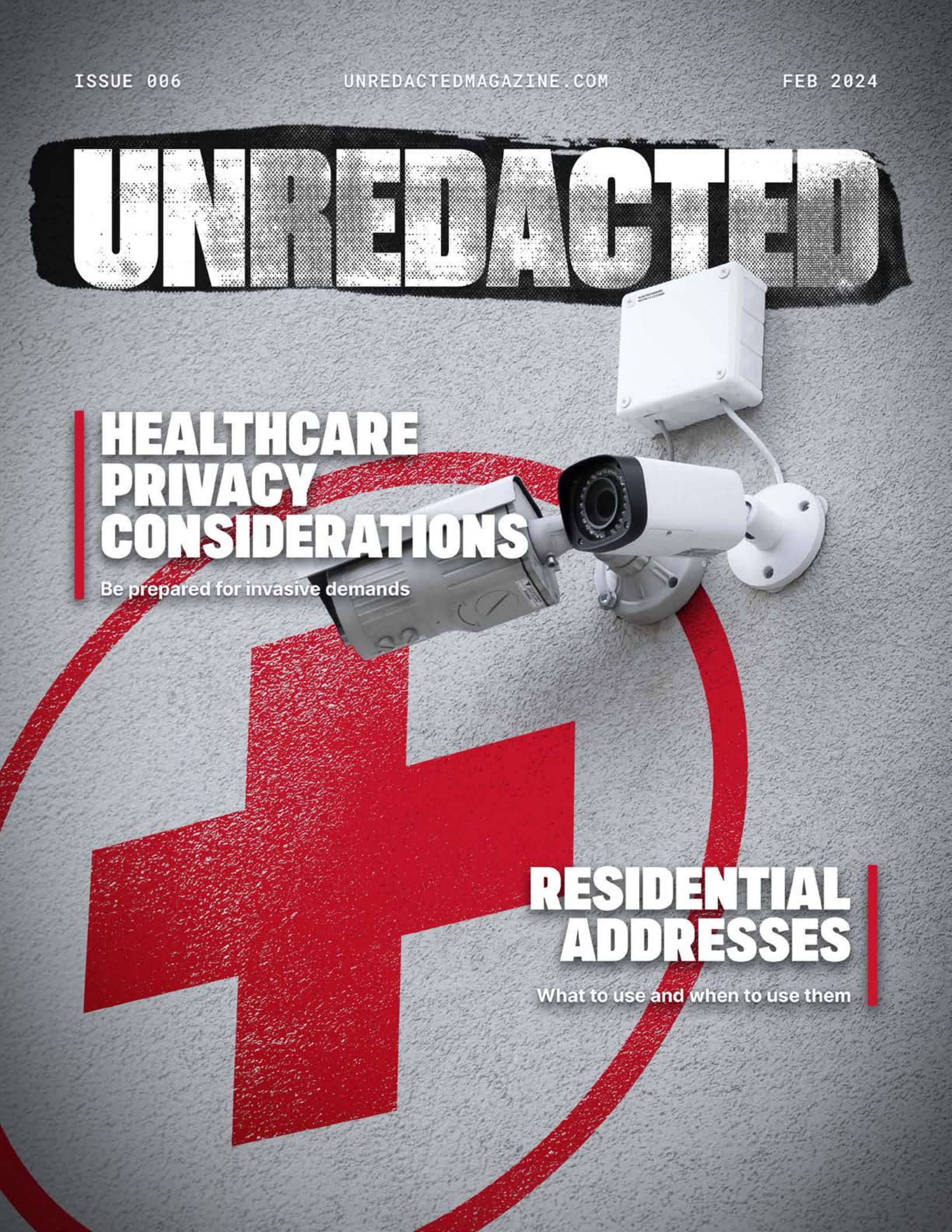
UNREDACTED

HEALTHCARE PRIVACY CONSIDERATIONS

Be prepared for invasive demands

RESIDENTIAL ADDRESSES

What to use and when to use them





**UNREDACTED
ISSUE 006**

IN THIS ISSUE

- 5** From the Editor
- 6** Healthcare Privacy Considerations
- 9** Cautious Streaming: Using Roku Players Privately
- 12** Address Confidentiality Programs
- 18** The Home Address Dilemma and Driver's Licenses
- 20** Product Review SLNT E3 Faraday Backpack
- 23** Wireless Security: Assessing and Minimizing Your Radio Frequency Trail
- 29** How your Apple account can be compromised with just your unlock PIN
- 32** Getting Ready For A Post-Quantum World Tuta Is About To Launch Post-Quantum Secure Encryption For Emails
- 34** It's Not Me, It's You: Breaking Up With My Cell Phone Number of 21 Years
- 37** Cat and Mouse Part I: The Attack Framework
- 39** The OSINT Corner OSINT Best Practices from the Client's Perspective
- 42** Hunting Apps for OSINT
- 44** Elastichunt: The Tool That Makes Database Hunting Easier
- 46** Cutting Down on Browser Extensions
- 49** OSINT Exploring With MealTrain
- 51** The Secret Privacy Benefit of a Costco Card
- 52** Polyglot Passwords
- 54** Looking Beyond the Numbers
- 56** Offline Life: DAPs Revisited
- 61** Reader Q&A
- 62** Updates
- 63** Privacy-themed Puzzles
- 64** Final Thoughts
- 64** Affiliate links

UNREDACTED is published free of any charge to the reader, and this file may be publicly shared in its entirety. All issues are available for free download at [IntelTechniques.com](https://inteltechniques.com). Contact details are also available at this site.

Copyright © of all articles belong to the original authors. The remaining contents of this publication are copyright © 2024 by UNREDACTED Magazine, and are published via a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International license. You may share it for free as long as you keep the entire file intact. Commercial use is prohibited.

Cover Design by Anonymous Reader. Layout by [Astropost](#). Special thanks to everyone who helped make this happen. You know who you are.



FROM THE EDITOR

By Michael Bazzell

It has been just over a full year since the previous issue of UNREDACTED Magazine. This is not due to a lack of interest from readers, but a lack of submissions. While things started strong after the first issue, the last couple of issues were a struggle for content. There were only three article submissions received between January and June of 2023. Therefore, I put no effort into another issue until recently.

For some time, I assumed the magazine was done. However, I could not stop thinking about future issues. I truly enjoy reading this magazine and I have found nothing like it anywhere else. We receive emails every day asking for more content. In January of 2024, I made another online push for content, which worked. The result is what you see here. I hope it continues.

The magazine is a community-driven product. Without the community driving it, it will go nowhere. If you would like to submit an article, please email it to staff@unredactedmagazine.com. If enough content is received, I will happily publish the next issue. Without content, there is nothing to publish.

I posted in January that sponsors were lined up to pay the costs and keep the content free, but this has sparked much controversy. We have received constant complaints about having sponsors. Most readers demanded free content without ads, which is unrealistic. Many readers only want ads from companies they already like, which defeats the point of advertisements. The moment we have an ad for a provider different than the one preferred by much of the community, the emails roll in threatening to never read another (free) issue unless we eliminate the current sponsor. I was even bashed online by the CEO of a company which competes with one of our previous sponsors for allowing anyone but them to place an ad for their type of product (which they declined to do). We can't please everyone.

The feedback from this post was overwhelming. Almost everyone encouraged us to run the ads and keep the content free, which we have done here. I sincerely thank our advertisers and encourage you to research their offerings. Without them, this would not exist.

This issue focuses more on long-form articles instead of numerous short pieces. I prefer these types of contributions. Please note that we try to edit these articles as little as possible. I always want to preserve the author's words, tone, and overall vibe. It is not our place to abbreviate their content or correct their writing patterns.

I sincerely thank you for the interest in this concept. I hope to meet back here very soon.

MB

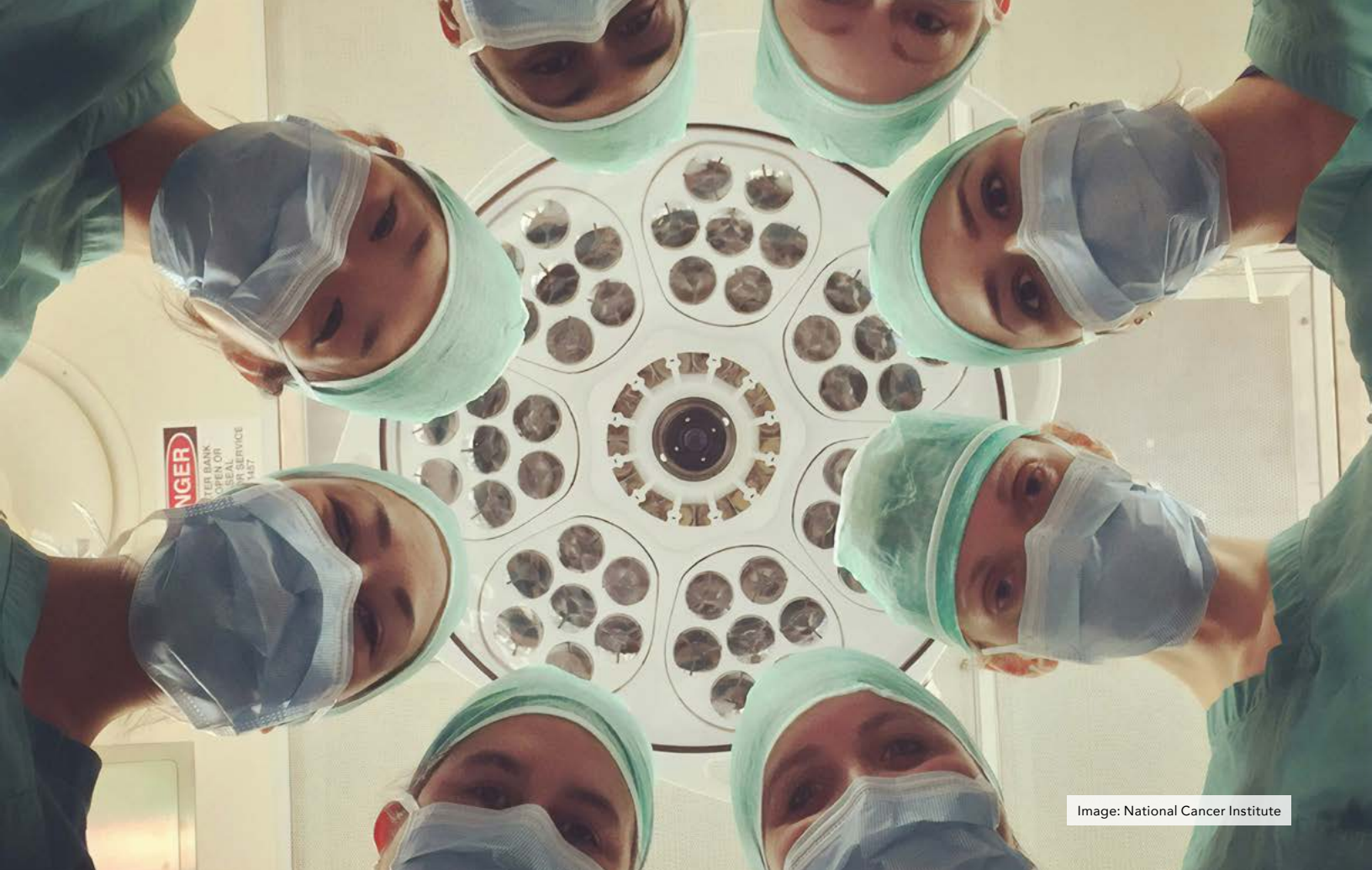


Image: National Cancer Institute

HEALTHCARE PRIVACY CONSIDERATIONS

By Michael Bazzell

Most readers have probably read about the latest ransomware attack against a cancer hospital. Not only did the criminals target a medical center, but they are also threatening to “Swat” patients undergoing cancer treatments with the intent of further disrupting their lives by sending police to their homes under the guise of an active hostage situation. This is a new low, but not entirely unexpected. This seems like a good time to revisit healthcare OPSEC. Coincidentally, I was overdue for an eye exam and overall checkup, so I decided to test my current plans for maintaining privacy while receiving healthcare.

The overall goal is to provide the minimal amount of personal information while not jeopardizing the level of healthcare needed. This is a balancing act. **I always enter every healthcare scenario with the assumption that any information provided will become public at some point.** Whether through a cyber-attack, data leak, or rogue employee, my data will be shared. It may even be intentionally resold. Therefore, I will carefully choose the information given to my provider.

First, there are a few things I will never give up, even if that means walking away. For me, this is my Social Security Number, my home address, a personal face photo for my file, and a copy of my government ID. The ID and SSN will be

abused in the event of a data breach, and a photo is invasive and unnecessary for my visit. My home address could be used in the next ransomware Swatting attacks. I will share my techniques for avoiding each.

Many years ago, our SSNs were used as driver's license numbers and health insurance account identifiers. Today, states create their own numbering scheme and insurance providers assign a unique number. In most healthcare scenarios, there is no benefit to the patient by storing their SSN in a provider's database. Some offices demand an SSN in order to either conduct a credit check to offer payment plans or provide to credit collection agencies if you do not pay your bill. An SSN is never required to administer healthcare. I provide my health insurance card (when appropriate) and pay my bills when they arrive.

While visiting my eye doctor, I was given the "new patient forms" which seem to pop up every other year. Once again, I was asked to provide a ton of sensitive details even though they already have most information from the last "new" forms. One line required an SSN. I left it blank and turned in the form. Before I was called back, the receptionist told me she needed my SSN. I told her that I was uncomfortable storing that in their Windows-based computer system because of the abundance of data breaches, which went over her head. She insisted and said that insurance companies require it, which is not true. I debated the laws for a while but she said they could not treat me until I provided my SSN on the form. I caved and tried something new.

This office is not a government agency and they do not verify any SSN given to them. In previous books, I have mentioned that SSNs such as 987-65-4321 will never be assigned to anyone, but they appear fake if scrutinized. Therefore, I gave her 666-12-9873.

Many years ago, the Social Security Administration decided that they would not issue SSNs which began with 666 because it was commonly believed to be the "sign of the beast". However,

I have no problem using it. You can give out any SSN which begins with 666 and not worry about abusing another person's number. The receptionist did not flinch, and had a new attitude of winning the debate.

If you do not want to provide an SSN beginning with 666, you have other options. Real SSNs never begin with the number 9 or contain 00 within the second bracket, such as 935-00-9822.

Next, she needed to scan my insurance card into the system. I had no issue with that. There is no sensitive information on the card. My name and date of birth are technically public information and can be easily found online. The address I use with my provider is a PMB where I do not live, and I provided the same address on all forms. The telephone number was a VoIP number which I reserve for healthcare in my true name. Then she needed to see my ID.

I do not object to displaying my ID for verification. This prevents healthcare fraud. However, I do object to them storing an image of my ID. I anticipated this and tried another new tactic. She originally asked for my driver's license, so I told her I do not drive. She then said it can be any government ID. I asked "Would my Department of State ID work?" and she confirmed that would be fine. I pulled out my wallet which was ready for the invasion.

This wallet has a windowed display section where I can place an ID and "flash" it to the receptionist. In the windowed area was my passport card. However, I carefully cut a thin strip of black electrical tape which covered "Passport Card" directly under "United States of America", all the way to each border of the ID. There is no law against this. This prevents the eye from focusing on the fact it is a passport card, and instead looks more like some other type of government employee ID. The bottom of the ID displays "Department of State" which falls in line with my previous statement. Did she think I work for the Department of State? I don't know, but I never said that I did.

She immediately said I would need to take it out of the wallet so she could scan it into the system. I told her it was actually against the law for me to allow her to scan a Department of State ID card, and even offered "Title 18, US Code Part I, Chapter 33, Section 701" for her to research. This time she caved and waived the requirement. I have also had previous success simply stating "I didn't think to bring it but I will next time".

Let's dissect this. If I had offered her an obvious Passport Card, but refused to allow a copy, this could have seemed like a weak argument. When I correctly referred to it as "my Department of State ID", that strengthened my defense against scanning. The very straight black line going all the way across the ID looked official and raised no eyebrows. I completed my visit, paid my bill, and left feeling as if I did not compromise any sensitive information.

The following week, it was time to see my nurse practitioner to explain my absence from my annual checkups. Shockingly, I was once again asked to fill out "new forms" which were now paperless. I was handed a tablet, which made me cringe. This brings up the paper vs. digital entry system. Years ago, I always preferred paper forms as they were often filed and forgotten. Today, it does not matter. If you print paper forms from a website and bring them in, someone is going to replicate every piece of data into the same system you would have used online. I have even seen some offices go to their own public website to type in the data from paper forms.

I believe there can be an advantage to submitting the data digitally yourself. If I write an SSN beginning with 666 on a form and someone types that in, they may become suspicious. If I enter the same number digitally and it passes validation, a human may never look at it. Since I never provide a true home address, cell number, SSN, DL Number, or other sensitive identifier to these offices, I do not have a huge objection to entering this online. Therefore, I provided my name, DOB, PMB address,

and VoIP number within the tablet, and in hindsight I should have done that online prior to the visit. That is where the data is headed anyway.

This brings up another consideration. Should you create an account within their "patient portal"? This is typically an area where you generate a new account and login credentials. This can be beneficial when you need to see lab results or communicate directly with your provider. It can also be another area to be breached by criminals. Some will say you should plant your flag and create an account before someone else does, and others will say you should avoid an unnecessary attack surface. I sit in between.

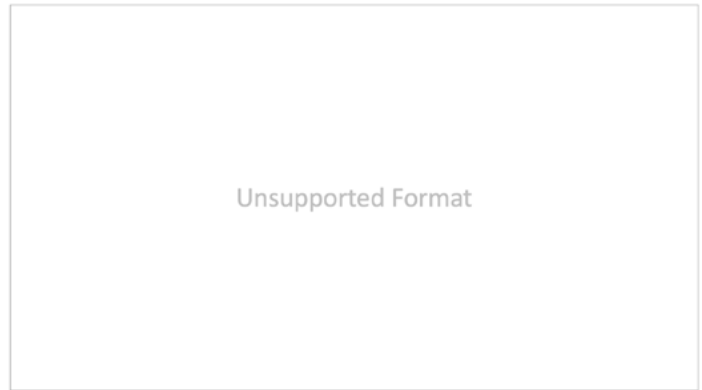
If I predict a future need to access a portal, such as to check results or make future appointments, I will create the portal account. I have one with my general practitioner. In the case of my eye doctor, I did not see a need so I declined to create the account. Consider your own situation carefully. You can never "undo" a portal account.

While on the tablet, I noticed new sections. They demanded my occupation, my SSN, and my marital status. I could not proceed until I submitted an option. If I selected "Single", I was allowed into the next screen. If I selected "Married", I was required to provide a spouse's name, employer, SSN, and DOB. This seemed odd and invasive. I found the simplest solution is to always say "Single" and move on. You can always provide an emergency contact later. I present a warning to readers without an understanding spouse. Entering "Single" can result in an uncomfortable conversation later.

I was able to complete the digital forms without much hassle. My profession was "self-employed", which I believe technically we are all working for our self in some way. The 666 SSN passed fine and my insurance details were already on file. I was brought back to get my vitals.

The assistant weighed me, checked my blood pressure, and did all of the typical things. She then said she would take a picture of me for my file. I balked and told her I was uncomfortable with that and she assured me that it would be securely stored in their system and they would never share it. I increased the resistance and told her that I would be soon undergoing facial treatments which might alter my appearance and that I have anxiety over the process. She quickly backed down. This was all true. I planned to wash my face later and I was upset that physicians now want to store pictures of us for no medical reason.

Since these visits, I have been playing with various online scheduling systems. Many offices now allow you to create your own appointment online and prompt you for the details which will be collected before the visit. I noticed that many of these demand you upload an image of your ID and insurance card. Again, the insurance card is no big deal, but the ID requirement bugs me. I recently had success uploading the following "Unsupported Format" image as my ID (created in PowerPoint).



The system only demanded an image, and it did not scrutinize the content. When questioned about the image error from my provider at check-in, I simply said "Don't ask me, I don't do computers very well". She said she would look into the problem.

In summary, I believe we should all be careful while supplying personal information to any healthcare provider, especially now that ransomware criminals are threatening to impact patients at their homes. These are my basic rules:

Name: I always provide my true name.

Address: I always provide a PMB or other CMRA address.

Phone: I dedicate a VoIP number for all healthcare.

Email: I dedicate an email address on a domain which I own for all healthcare.

DOB: I always provide my true DOB.

SSN: I never provide my SSN. When forced, I give them a non-existing number.

Family: I never provide family member names, addresses, phone numbers, etc. I always provide the VoIP number of a trusted person as my emergency contact.

Insurance Cards: I always allow scanning of my full insurance card.

Photo ID: I offer to display my ID to them, but I never allow them to scan it.

Online Form Completion: Today, I prefer to complete all forms online for less scrutiny of my information.

Portals: I try to avoid any healthcare portals which do not offer me a direct benefit.

Apps: I avoid all healthcare mobile apps completely.

Please remember that health is more important than privacy. Never jeopardize your health needs for the sake of being anonymous. ■

CAUTIOUS STREAMING: USING ROKU PLAYERS PRIVATELY

By anonymous

Roku streaming players are now abundant across many households. Just like any other device connected to the internet, they present new privacy challenges that we want to mitigate. The best option would be to abandon using streaming services and players altogether, but some of us are unwilling or unable to do so. This article will help you lessen the privacy risks when using a Roku streaming player. While creating this article, I used a Roku Express 4k+.

First, we will create a new anonymous Roku account. Next, we will physically remove the microphone from the Roku remote. If you have a brand-new Roku streaming player, you can skip to the first-time setup section and continue from there. If you already have a Roku streaming player and would like to improve your privacy while using it, you can still follow these steps after factory resetting your device. Navigate to Settings > System > Advanced System Settings > Factory Reset on your Roku player to reset it. Be prepared to sign in again to all of your channels and services. After factory resetting, delete your old Roku account by signing in to roku.com and navigating to My Account > Delete Account.

First Time Setup

Creating an anonymous Roku account from the beginning is important for

increasing your privacy. To start, connect your Roku player to your TV and make selections in the setup menus. You will arrive at a screen prompting you to connect your Roku to the internet. For extra privacy, use a router with VPN software installed on it. Connecting your Roku to a VPN router will allow you to avoid revealing your true IP address. However, some streaming services will block users that they detect are using a VPN. Getting blocked will depend on what streaming service and VPN provider you use. If you are blocked from streaming, you might have to connect your Roku to a network that does not have any VPN protection. I suggest trying to stream using your VPN router first, and only switch to the unprotected network if you are blocked.

After pairing your remote and connecting your Roku to the internet, you will face a screen demanding that you sign in with a Roku account. Do not enter your email address yet. Use a separate computer to create the account.

Go to Roku's signup page at my.roku.com/signup and begin the account creation process. Use an alias email and a pseudonym. I had no issues when I did this behind a VPN. Next, you will be required to link a payment method to the account. Roku says there are

no charges for account creation, and linking a payment method will allow you to purchase subscriptions to different services. However, my streaming services are already paid for directly, and I don't need Roku to be a middleman. Once you click "continue" after entering the name and email information, your account is already created. You can close the payment screen and then use your account like normal, even though Roku says payment information is required.

Go back to your Roku player on your TV and select "Enter Email Address." Enter the email address you just used for creating the new Roku account. You will need to click a confirmation link sent to that email. Upon opening the link in the email, Roku will ask for a device name and what room the Roku player is in. I selected "Living Room" because I guessed that's the most frequent selection. Change the device name to something generic and unrevealing. After clicking continue, Roku will ask for a payment method again. This time you will see "Skip this step" at the bottom. Click that and move on. Make channel selections and click continue through all of the following pages to finish the confirmation process.

You now have an anonymous Roku account linked to your Roku player. I would like to draw your attention to

some important settings in your Roku player. Use your TV and Roku remote for these changes.

Settings > Privacy > Advertising, uncheck "Personalize Ads"

Settings > Privacy > Voice > Microphone access > Channel microphone access, select "Never Allow"

Settings > Privacy > Voice, uncheck "Speech Recognition"

Roku Microphone Removal

As of the writing of this article, there are 3 types of Roku remotes: the Roku Simple Remote, the Roku Voice Remote, and the Roku Voice Remote Pro. The voice remotes have a microphone used for searching content via spoken commands. It is activated by holding the microphone button (on newer remotes) or the magnifying glass button (on older remotes). If your Roku remote does not have a microphone or magnifying glass button, then you have a Roku simple remote. Roku simple remotes do not have a microphone.

Most people leave their Roku remotes ready for easy access in the middle of a room. If they have a voice remote, this means they have placed a microphone connected to the internet in the center of their room. It could potentially record any conversation happening in that room. Roku's settings do not allow you to completely disable the microphone.

I do not ever use the voice search function, nor does anyone in my family. I find the "Search" function on the Roku home screen to be perfectly usable, even if it takes a few seconds longer to type with the on-screen keyboard. If you are like me, I see no reason to keep the microphone in the remote. You may be able to purchase the Roku Simple Remote and use it instead, but it is not compatible with all Roku players. For instance, it is not compatible with my Roku Express 4k+. You could also try getting a universal remote that doesn't have a microphone, but some universal remotes are only partially compatible with Roku players. Therefore, I suggest

physically removing the microphone from the remote as a quick and free option. I will explain the removal steps below.

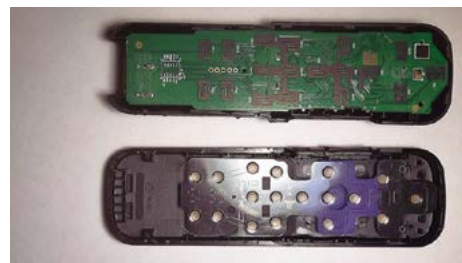
Newer Roku voice remotes have a microphone pinhole below the power button. Older Roku voice remotes have the microphone pinhole to the left of the power button. Take note of where this pinhole is, because the microphone will be behind it.

The disassembly process of different types of Roku remotes varies slightly, but the general steps are the same. For additional guidance, a search of "Roku remote teardown" will yield other videos and tutorials of taking apart a Roku remote. However, I could not find any tutorials that specifically demonstrate the microphone removal process. In my pictures, I have a Roku Voice Remote (not the pro version).

Start by removing the battery cover and batteries from the remote. Using a small flathead screwdriver or spudger tool, gently pry the back of the remote casing apart along the crack running down the side. You will hear a click as you pop each plastic snap out of place. In this picture I have begun the process of prying it open.



Separate the two halves.



Remove the green circuit board. Locate where the microphone pinhole would be when the outer casing covers

the circuit board. On my remote, it aligned with a small gold box with another pinhole. Inside this gold is the microphone. It is labeled U5 on my circuit board.



Using needle-nose pliers, pinch the gold box and twist it off. Go slowly and don't yank it. Underneath the gold box, you might encounter an additional black piece with small circuitry on it. Pull this piece off as best you can too. Once these pieces are off, only the silver contacts should be left behind on the board.



Reassemble the remote by setting the board back in the casing and clicking the two halves together.

If you have unfortunately broken your remote in this process, you can purchase a new remote from Roku or try a universal remote. After assembling the remote again, make sure all of the buttons still work. When I now hold the microphone button on my remote, the microphone icon appears on my TV expecting me to speak. Even when I scream into the remote, it now always says, "Unable to hear you. Try again."

If you have followed all of this, I commend you. You now have a more private Roku setup. Perhaps the only way to go further would be to throw away your Roku altogether. ■

WHAT DO YOU REALLY KNOW ABOUT YOUR DIGITAL FOOTPRINT?

Reported at: 19/01/2024 09:36:37 Export PRO

Networks **10** Data breaches **17**

Overview

mark.zuckerberg@gmail...

- ASKFM
- GARMIN
- IMAGESHACK
- NOTION
- SKYPE
- CHESS.COM
- FACEBOOK
- FOURSQUARE
- GOOGLE
- LINKEDIN
- ABOUT.ME
- FLICKR
- GRAVATAR
- MOCOSPACE
- PICSART
- RUNKEEPER
- TARINGA

Google

| | |
|-----------------|---|
| User id | 104560124403688998123 |
| Email | mark.zuckerberg@gmail.com |
| Image | |
| Maps url | https://www.google.com/maps/contrib/104560124403688998123/re... |
| Calendar url | https://calendar.google.com/calendar/u/0/embed?src=mark.zuckerbe... |
| Google plus url | https://web.archive.org/web/*/plus.google.com/1045601244036889... |

LinkedIn

| | |
|-------------|---|
| Username | Mark Zuckerberg WhatsMyName |
| Link | https://linkedin.com/in/mark-zuckerberg-618bba58 |
| Firstname | Mark |
| Lastname | Zuckerberg |
| Bio | CEO at Facebook |
| Actual work | Facebook |
| Location | Palo Alto, California, United States |

Sign up and get **one free month** with code: **URDCT**





Image: Timothy Eberly

ADDRESS CONFIDENTIALITY PROGRAMS

by **Lucky225**

As a privacy advocate I have always been very conscious of the ways pieces of information tie together. For example, if you have someone's phone number, it's very easy to find out their address from it and vice versa. Throughout my life, I have employed various strategies to separate my public identity (i.e. name, dob, ssn, phone number, etc.) from my true fixed residential address. However, we all make mistakes and we also can't control how the other loved ones in our lives handle their personal information. As a result, my family has been the victim of "swatting" threats in the past and while my family is a "victim" of this heinous crime, it was in a way a blessing as it has qualified me as a victim of stalking to participate in State funded "Address Confidentiality Programs" or ACPs — Sometimes called "Safe At Home."

So what exactly is an ACP? It varies from State to State, but it's basically a State run program that allows victims

of certain crimes (usually Domestic Violence, Sexual Assault, Stalking and Human Trafficking) to receive mail at a mailing location the State provides where they forward the mail to your own mailing address free of charge. This mailing address is often referred to in the statutes and by the ACP programs as a "substitute address."

Additionally in most States every local and State government agency in the State is required to accept the "substitute address" whenever and wherever a residential address is required, with very few exceptions. Some allow you to use the substitute address or another fictitious address as the true residential address on your ID or Driver License and vehicle registrations, others may require the real address but suppress it after the fact. Many allow you to register as a confidential voter so that your address is not publicly available even on voter rolls to the political parties. Some have special

protections for real estate transactions and some have privacy protections that allow you to demand your information be deleted if posted on the internet or in other public spaces.

I've had the unique ability to observe how many of these States run their programs as I have personally participated in California, Colorado, Pennsylvania, and Texas' ACP programs. I also know others who were victims of swatting who have enrolled in Arizona, Massachusetts, and Minnesota's programs. I'm going to detail some notes on each of these State's programs and compare them against each other, the way these programs are ran by each State is wildly different and so if you're a victim and thinking about moving out of state to one of these States perhaps this guide will help you in your consideration as I wish someone had prepared such a guide for myself.

ACP substitute addresses

The first thing you may want to consider is what type of mailing address the ACP provides their participants to use. If you're familiar with the difference between PO boxes and PMBs, you likely want a PMB style mailing address. Colorado and Arizona offer these types of physical addresses for use as a substitute for your true residential address. In my opinion these 2 states offer the best ACPs in the nation and should be a uniform model for the other ACPs, Minnesota would probably edge out as the best program IF they used a physical address instead of a P.O. Box. Most States, unfortunately, only provide a PO BOX substitute address. This includes California, Massachusetts, Minnesota, Pennsylvania, and Texas.

Eligibility

This will vary greatly from State to State. Most States include victims of domestic violence, sexual assault, and stalking or harassment. However, some States only include domestic violence victims as their legislation was patterned over California's oldest law which didn't initially include other victims. Some states require some form of evidence to support your claim (such as a protective order, police report, etc.) while other States only require a statement. Minnesota is the easiest state to qualify for as they allow any "person [who] fears for the person's safety". See 5B.02(e) to apply regardless of if they're an otherwise qualified victim or not. Most states require you to meet in person to complete an application, while States like Pennsylvania and New York allow you to apply directly electronically. Most States require you to be a resident. Pennsylvania is an outlier that allows you to apply regardless of if you're a resident or not, more on that in the Nomad section of this article.

Driver License, Identification Cards and Vehicle Registration

The next thing you likely wish to consider is how driver's licenses or ID cards and vehicle registrations handled. Colorado and Arizona again win on this,

you just use your physical substitute mailing address and no proof of residency is required when presenting the ACP card which serves as your proof of residency. You do have to provide a physical address in Colorado for vehicle registrations for taxation purposes, however they simply look up the tax rate first and then save that to your vehicle registration profile, the true address itself does NOT get saved as any part of the vehicle registration record.

Massachusetts has a similar procedure, though because they use a PO BOX, the RMV has agreed to allow these participants to use the RMV's main Boston branch address as the physical address on the license, while it gets mailed to the ACP PO box. The individual I spoke to who is familiar with this process was not pleased with this since obviously they can't get mail at that address and many entities want your driver license address to match your residential address for verification purposes.

He found that by using the post office's physical address he could receive mail to the PO BOX using the USPS street addressing for PO box service. This is despite the fact that the USPS insists you sign a form to use street addressing. They usually deliver mail anyways as they have no way of keeping track of this when delivering actual PO box mail.

He attempted to use the Massachusetts' ACP's post office physical address to get his driver license, and he was successful, but then the RMV revictimized him and accused him of lying about his residence address, a crime of 'false application' for a driver license. He had to have an RMV hearing to keep his driver license from being suspended. In the end, since the Massachusetts ACP and RMV only allow using an RMV branch address that you can't receive mail at, which for a host of reasons is very wrong (i.e. if you get in an accident and exchange information, if you're suspected of some sort of driving violation and the police send mail to that address, etc.) I

have to give the MA ACP a fail on this one.

Most other States simply let you use a PO BOX on the driver license, this includes California, Minnesota, Pennsylvania, and Texas. As far as I know from participants I've spoken to, no proof of residency is required. I'm not 100% sure on how Texas is supposed to work in person as the program was new at the time and I changed mine online in Texas when I was there by using the ACP victim ID number as the first part of the PO BOX address which bypassed their PO BOX checking, but I'm told you should just have to show your card to the TXDMV clerk now. Vehicle registrations in Texas also only requires the PO BOX, and when I was a participant back in 2009, they were trying to require your "vehicle location address" but I was able to get their registration manual updated to provide "Any transaction involving an ACP participant may use this post office box number instead of any physical address the department may otherwise require."

California unfortunately is a bit of a mixed bag when it comes to protections. You have to provide your true residence address to their DMV, as well as proof of it. This is especially challenging if you have employed measures to ensure there is no proof your identity resides at your true residential address. You can use the PO BOX address they provide you as mailing when you get your driver license and registration, but your true residential address will be in their database and accessible to anyone who has a permissible purpose, such as law enforcement, vehicle insurance providers, toll road authorities, etc.

Furthermore, California is an automatic voter registration State so you need to affirmatively OPT OUT of voter registration. California's Safe At Home ACP program does NOT inform new participants of this and undoubtedly some participants will end up in the public voter registration unbeknownst to them.

After your driver license and vehicle registrations are issued, you can

request suppression through the DMV's confidential records unit (CRU). This suppression actually 'seals' your driver license and vehicle registration in a manner where nobody can access it without calling the Confidential Records Unit, and unless it is law enforcement they will call you to ask if they may release your records (i.e. if you're getting vehicle insurance). The form also says to notify the CRU if you have concerns about law enforcement accessing your records (i.e. if you're a domestic abuse victim with an ex-husband that's a cop, you may want to know when LEOs request.)

In some respects, this is stronger than protection offered in other States, but in many respects it's a failure, especially if you have just moved to California from out of State. If you already have a CA license or ID and registration you can just mail the form to get the suppression added without going into the DMV to tell them your new address, but if this is an original application you have to go through the normal DMV processes first which may expose your residential address for a short period of time. In my opinion this Catch-22 is a failure on California's Safe At Home ACP program, as the program has been around since 1999 and they have not yet addressed this issue that other States handle seemingly without requiring the true address in most cases. Even after you suppress your records, whenever you get a new vehicle and have to register it you would be exposing yourself again before you can suppress the new vehicle registration.

Nomads and those that reside in States without a program

If you're a nomad, or if you live in one of the 12 or so States that doesn't offer an Address Confidentiality Program, but you're also a victim, Pennsylvania probably offers the best solution here. Furthermore, even if your state offers one of these programs, enrolling in Pennsylvania's program can help add another layer of obscurity as to the actual State you are residing in. Perhaps your state's program is so poorly ran that PA's will actually benefit you. Pennsylvania's program is unique

in that they offer this program to Out of State residents. Specifically, Title 37 of the Pa. Code § 802.3 provides:

(d) Commonwealth residency is not a requirement for ACP participation. ACP applicants who do not provide a Commonwealth residential address will be enrolled as a "Non-PA Resident." This designation will appear on the ACP participant's ACP authorization card.

Pennsylvania provides a nice pretty letter that you can give to any financial institution that explains the physical address can be used in the residential address fields, but that mail must go to their PO BOX. Why my State can't produce such a letter for me is beyond me, I've tried to get them to do so but they refuse to. This is a huge win if you're a victim and also a nomad. For example, if a bank gives push back on a South Dakota nomad PMB address, you don't really have a lot of recourse. However, if you're a PA ACP participant, you can cite an actual FINCEN ruling and can provide the PA ACP letter from their Office of Victim Advocates that cites the law and that they must accept the address. Presumably a South Dakota nomad who is a victim would be able to enroll in the PA ACP using their PMB residential address, though admittedly I am not a nomad so I have not tried.

In addition to this Pennsylvania's ACP was easy to enroll in, you can do so remotely, electronically and all via e-mail. A sworn statement was all that was required to prove I am a victim. I would however caution, please only apply if you are an actual victim. There are criminal penalties for making false statements.

If you are a nomad and a crime victim in Pennsylvania this may also help getting an ID or Driver License for free even if your current ACP card reflects a NON-PA resident, assuming you are moving into PA to flee abuse. Homeless individuals are entitled to free ID in PA, and their fact sheet about it provides the following—For purposes of application, you are "homeless" if you are an individual who:

is fleeing, or attempting to flee, domestic or dating violence, sexual assault, stalking, or other dangerous or life-threatening conditions for you or that jeopardize children in your current housing situation, and you have no other residence and lack the resources or support networks to obtain other permanent housing.

I am not a lawyer, and this is not legal advice, but presumably even if you establish a permanent residency in PA after the fact you could keep that PA ID or driver license without having to do anything additional as you are an ACP participant and the PA DMV is required to accept the ACP address which you would have already provided them when getting the ID.

Voter Registration

Most States offer a confidential voter registration for their ACP participants. I don't want to get political here, it's great that States offer this confidential procedure, but as the late Justice Scalia once was quoted as saying, "Some things in life are more important than votes."

I would caution participants who wish to register to vote. You definitely will need to provide your physical address as voter registration requires this to determine what voting precinct you belong to as well as which local city and county elections you're eligible to vote in.

In Colorado each county is responsible for handling ACP voter registration, and often times the clerks would not perform this correctly. The voter registration NAMES were masked with an ACP participant ID number, but this number is technically not confidential and can be reversed to the participant through an open records request and in any case even if it were confidential information, the counties were previously leaking information about your location, while the address of record was your ACP mailing address, this address itself has an apartment number unique to you and the registration itself would reveal your precinct information and

in some cases your personal phone number. They finally stopped making these records publicly accessible a few years ago, but the experience left a sour taste in my mouth, and the fact that voter registration is just another electronic database, I don't trust that a data breach wouldn't reveal someone's confidential voter registration.

I have not researched other States much further in this regard as I just don't have any intentions on ever registering after my previous experiences, they do all have similar but different processes though. For example, California requires you send the confidential registration application directly to the Secretary of State instead of going through the county, however they end up remailing this directly to your county clerk who may not be aware of the Safe At Home program and one misstep could accidentally not mark your voter record confidential correctly.

Minnesota probably has the strongest protection. Their process involves the Secretary of State who runs the Safe At Home program working as an intermediary. The county voter registrar only receives certification that you are eligible in that county without the actual address and when a ballot is sent it is also returned to Sec. of State who verifies the signature and then sends the ballot back to the county certifying the ballot is valid and legitimate.

Utilities

This is the one where I think Colorado really wins. They have agreements with Comcast, CenturyLink, Xcel and Colorado Springs Utilities (CSU) to allow participants to sign up in alias names with no credit checks. This will highly depend on where in Colorado you plan to move to, as certain electricity providers are not covered (at least they weren't when I lived there, but Colorado's program is constantly changing to meet challenges.) I would highly suggest Xcel or CSU serviced areas as these utilities never leaked my true information. Comcast unfortunately leaked my true address once from IP and my alias name and phone numbers on the account did

show up on whitepages.com alongside the service address on the accounts. But that said, Comcast cable modems work anywhere in the State of Colorado regardless of the service address on the account, so if you're creative enough you won't need to sign up with your true address to begin with, however the allowed use of alias name without credit check is beneficial. No other ACP has similar utility protections that I am aware of.

Real Estate

Almost all ACPs offer the ability to suppress your property record(s) in one way or another. In Colorado I was able to get the county to even change the grantor/grantee names to SEALED, however when I sold my house the county said that was no longer the correct practice, the names are now searchable, which really is a shame since if you know the date of the sale and the grantor's name you can then search the grantor's name in the same county to easily find the property that was sold, but I digress. The property tax record itself however won't be available online and this goes the same for Arizona, so these 2 States offer strong protection. I would just offer guidance that names (even if not associated with property address) should not be searchable on the county clerk & recorder's website (ie in a grantor/grantee index) or it's a useless protection. Otherwise, if a stalker knows who sold you the house they can get the previous deed information when it was granted to the seller to reveal the true property address.

California offers the ability to replace the property address with the PO BOX, but I'm unsure how well that will work out in practice if the APN/PIN and legal description is still available and suffers the same problem of names being searchable. Counties I've spoken with have no procedure on how to handle this. Some will sell your deed information within a month of it being recorded directly to data-brokers along with all the other deeds for that month. California does have a law however that a participant can demand that a person not disclose his or her home

address on the internet, and its use of term-defined words "publicly post or publicly display" seems to imply that would mean the ability to obtain the home address without the address itself necessarily being posted.

Cal. Government Code § 6208.1 provides:

(b) (1) No person, business, association, or other entity shall knowingly and intentionally publicly post or publicly display on the internet or other public space the home address or home telephone number of a participant if that individual has made a written demand of that person, business, or association to not disclose their home address or home telephone number. A demand made under this paragraph shall include a sworn statement declaring that the person is subject to the protection of this section and describing a reasonable fear for the safety of that individual or of any person residing at the individual's home address, based on a violation of subdivision (a). A written demand made under this paragraph shall be effective for four years, regardless of whether or not the individual's program participation has expired before the end of the four-year period.

Subsection (f) further provides the following definition for "publicly post or publicly display":

(3) "Publicly post" or "publicly display" means to communicate or otherwise make available to the general public. (Emphasis added).

Per Cal Gov Code 6209.5 participants can protect their address by placing it in a trust, however your mileage may vary in attempting to enforce this (and the other Cal Gov Codes), even if you close in a trust the county may still list your name as trustee in the grantor/grantee index. I would strongly recommend considering other options such as an anonymous trust with a trusted third party such as an attorney as trustee of the trust.

Notwithstanding these issues, Minnesota does offer what is likely the

greatest protection in this area as their law also requires all 3rd parties involved in the purchase of the house (seller, bank/mortgage, title plant companies, etc.) to not disclose your property address to any third party and to use their PO BOX as the only address of record, they also have a clear-cut process on how the counties are to deal with this situation.

Names and alias usage

Some States, like California, allow you to petition the court for a confidential name change. California's is particularly interesting as the name change order only shows the new name and not your previous name. The US State Department has a whole section about this for Passport issuance. However, I don't recommend name changes unless you have a clear-cut path, they will almost always tie back to the original name via your credit report when you update accounts, etc. This option should only be exercised if you're creating a brand-new identity, including getting a new SSN and ensuring the new SSN is issued in the new name only.

Most States unfortunately will require one 'legal name' even though there is no such thing as a legal name in most States and federally. In Pennsylvania it took a month's long battle with the program consulting with their legal department in order to accept my multiple names that I use legally as common law. California's program insists on using ONLY one name and will return any mail not addressed in the 'correct' name. This is my experience in other States as well. I think this is a horrible policy. Victims need resources and the use of alias names to escape abusers is common. If you get married or divorced or otherwise change names it also becomes another hassle for victims because if you don't update every institution (an almost impossible task) with your new name mail intended for the victim gets returned with no notification to the victim.

Colorado let me use more than one "legal" name, but would not allow mail for a business name, which may

be important to you if you're a sole proprietor or work from home and own a business. Ironically, Colorado will let you use an alias name on your utilities and forward mail from utilities addressed in an alias name while simultaneously not letting you use other names on other mail. Many of these States explicitly state in their statutes that the substitute address may be used in place of the participant's true residential, school or work address yet won't allow mail addressed to your work. Inquire with your ACP if this is a concern to you.

Banking

There's no federal law that requires banks to accept an ACP address, however FinCen guidance has been issued on the matter. This is again where States like Arizona and Colorado win, because they provide a physical address, which is also on your ID. You may never have to interact with bank employees to explain your situation.

In States that use a PO BOX it gets complicated because the guidance states, "Therefore, a [financial institution] should collect the street address of the ACP sponsoring agency for purposes of meeting its CIP address requirement." This requirement is immediately met in States like Colorado where your ACP mailing address IS the street address of the ACP sponsoring agency, while California on the other hand has offered a convoluted process that relies on the bank knowing to contact Safe At Home who will give some "secret" address to the bank instead of just trusting their participants to use this address as residential address only and the PO Box for mailing without having to contact Safe At Home. It's in my opinion a stupid policy where the program distrusts their participants to not accidentally use it for mailing, but in reality, the participant could obtain this address from their online bank account which will show the address after the bank collects it. So why not just give your participants the address and explain they must ensure mail isn't sent there? Or better yet, why do these programs not convert their PO Boxes to Street addresses using the Street

Addressing for PO BOX service that USPS offers?

From personal experience, I just had to have my privacy.com account reinstated. In spite of the fact that privacy.com does not have telephone representatives, California insisted that a phone call must happen with the financial institution and refuses to change their policy. I was able to enroll in Pennsylvania's program and receive a letter from them and provide that to privacy.com to reactivate my account in lieu of California's procedure over a weekend, so I am enrolled in 2 programs just because Pennsylvania literally runs their program better than my home State, one of many reasons I'm moving.

That said, I'm told Wells Fargo honors address confidentiality programs and collects only the PO BOX information (if your ACP uses a PO Box) when a card is presented. In practice I wasn't able to do so easily in the branch. However, they did accept my PA street address (that mail cannot be sent to) which the program gives as my residential address while using my PO BOX as my mailing. Another individual who actually had them follow procedure showed me that when ACP protections are on the account, they won't let you sign up for credit cards from your login, instead directing you to call a special number, so there is definitely a process. My local bank didn't seem to know or care about it though so your mileage may vary if they know how to get it set up correctly or not. I've also used the PA ACP process to establish stock accounts at Fidelity (after threatening a FINRA complaint), establish credit cards and take out a personal loan from Discover.

Schools

Almost all of these programs have a process for enrolling your children in school. Colorado's was great, they facilitated transfer of records from old school to new and never revealed the true address to school officials, only a letter declaring that they have determined you are eligible to enroll locally. I can't speak for other ACP's

processes as I have no other experience with this.

Security Screening

Some States, like Colorado, have their mail screened through an x-ray machine, metal detector and other methods to ensure there are no harmful substances or other items. With the rise of Apple Airtags, this may be a concern to you, especially if you do not have your own PO BOX or other maildrop to receive mail at, and your ACP forwards directly to your residence. By the way, if you DO have your own mail drop I strongly recommend opening ALL MAIL upon pick up BEFORE leaving the post office to screen for this type of stuff as standard OPSEC. I brought up the Airtag concern with Colorado while I was there and this is how their mail screening employees responded to ACP staff:

Yes, someone could send one of these in the mail, along with similar app-based tracking devices. Such is one

of the reasons why we refuse anything bigger than the standard envelope or pouch for ACP participants. Our metal detector will indicate anything that is organic, metallic, or ceramic; so, it should show up on a regular scan. These also have batteries in them, so it would be visible to the detection unit (we can see something as small as a tack or paperclip). I will copy all of my staff on this to remind them to remain vigilant on their screening procedures.

Colorado however is unique in that ACP mail goes to the State's mail processing center where ALL State mail is screened. Many ACPs using a PO Box at the Post Office likely do not do this additional screening and if this is a concern for you, you may wish to consider moving to a State like Colorado.

ACP software and Data Breaches

Like everything else, it should be noted that State governments are no stranger to data breaches, and

unfortunately at least one State has suffered from a data breach that exposed ACP participant information. Upon information and belief, that particular State was using software advertised in the NACAP (National Association of Confidential Address Programs) newsletter. Ironically, this particular State cautioned participants to not use email to modify their applications (i.e. when moving to a new address, adding a new participant, etc.) and to use USPS mail to mail back their applications because email was "not secure." This same State then proceeded to scan and save these applications in a digital format on computers connected to the internet! Their agency then suffered a ransomware attack and several ACP participants docs were exposed including fully scanned applications, scans of their driver licenses, scans of the evidence to support their eligibility. It may be prudent to ask your particular ACP agency how they handle and store application data since you will have to provide your true address and other information to enroll. ■

THE CYBER WAYS PODCAST

Translating academic cybersecurity research into real-world application

Hosted by Thomas Stafford, Ph.D. and Craig Van Slyke, Ph.D.
of Louisiana Tech University
and the
Center for Information Assurance



business.latech.edu/cyberways





Image: Kindel Media

THE HOME ADDRESS DILEMMA AND DRIVER'S LICENSES

By Rob Hoffman

In my Unredacted Magazine article of June 2022, "The Home Address Dilemma and Form I-9," I documented the challenges and possible solutions for filling out the form that allows one to work legally as an employee in the U.S. Many government agencies and their forms present privacy challenges, and those of the DMV (Department of Motor Vehicles) are no exception. I will share my recent experience in applying for a new driver's license in New York State.

There are three options for a NY State driver's license: "REAL ID," "Enhanced," and "Standard." According to the NY DMV, starting on May 7, 2025, if you wish to use your DL as ID to fly domestically, or enter a military base or certain federal buildings, the REAL ID will be required. A REAL ID is not necessary for any of those things if you

use a U.S. Passport, but some people like the convenience of not having to carry a passport.

To renew your DL in NY State (in any of the three formats) requires a lot of proof of your name, citizenship, and address. Suffice it to say that if you want a valid DL, there is no way around giving the DMV the correct and proper information if you are to follow the law. They don't mess around at the DMV, and I don't suggest messing with them or lying on any government form. I decided at first to get a REAL ID, which I now regret because I didn't need it. Since I was able to get my P.O. Box on my last DL, I had hoped to do the same this time.

Unfortunately, the new policy in NY is that only your true physical residential address can be on your REAL ID DL. They have gotten more stringent, clearly, because the REAL ID, even

though it is a NY State document and not a federal one, is something deemed acceptable by the DHS (Department of Homeland Security).

Once again – they don't mess around. And here's the sobering reality: in order to tell the truth AND prove it (especially for the REAL ID, which requires more proof of name and address than a standard DL), the address on the documents I provided (rental lease and bank statements) had to be real and had to match what I was giving to them. Therefore, I had to update my address at my banks (which until this point had CMRA addresses on record). The downside of this is that when you change your address with banks, they send this information to the credit bureaus. I fully accept the ramifications of that. If I could do this all over again, I would have initially applied for a "standard" license, and I would have given them the documentation from

the financial services company that already had my real address (required for renter's insurance – and it's an institution that I believe kept that information from the credit agencies).

A few days after receiving my REAL ID DL, I changed my mind – I was not comfortable with my residential address on my DL, so I went back to the DMV and downgraded it to a "standard" ID. They allowed me to put an alternate address on the DL (YAY!), but it could not be a P.O. Box (WOMP-WOMP). However, I realized that I could use the "street address" version of my P.O. Box (which many USPS stations give you in order to receive packages from FedEx, UPS, and the like who cannot deliver to P.O. Boxes). I suppose you can also use a CMRA or other mailing address. The only downside is that I will continue to need to have my passport to fly anywhere or to enter government buildings. (Fine with me!)

An "Enhanced" ID, whose requirements are as stringent as the REAL ID, allows you to fly domestically

but also to return by land or sea to the U.S. from Canada, Mexico, and some Caribbean countries (It cannot be used for air travel between these countries – a passport would still be required for that). I have no use for those features, so I opted for the "standard."

Although I carry my DL around all the time, I use my passport for ID (The only place you actually need a DL is at car rental agencies). There is an NYC office building I go to frequently that asks for (and scans) DLs upon entry. I show them my passport instead. They can't put it into their scanner, so when they ask to take a photo of it with their little desk camera, I let them do it, but I deftly cover some or all of the passport's ID number. No one has ever noticed that or complained. I feel that little trick gives me a bit of protection. As Michael has often said, privacy is a marathon, not a sprint. I would add that privacy is occasionally a huge victory, but most of the time it's a lot of tiny little daily ones.

So, what's the big picture as far as physical address privacy is concerned? Naturally, check the rules of your state or territory. For those people willing and able to achieve "nomad status," it's quite possible to avoid giving out your actual physical "where-you-really live" address, but for most of us on-the-grid people who live in one place, and want to legally drive (at least in NY State), you should expect to give up certain information (I suspect my passport renewal will be a similar experience). But for the DL, having an alternate physical "mailing address" was very useful, and choosing the "standard" option requires slightly fewer forms of address proof than the REAL ID.

One other note: I often use my expired passport for ID. Not for flying, employment, getting into government buildings, or anything official — I just use it for getting to a bar or club. It's not illegal as far as I've read, and no one has ever questioned it. That way, if anyone tried to steal that passport number, it wouldn't matter because that number is invalid. ■

FORTIFY
24x7
Cybersecurity Managed™

MDR | XDR | INCIDENT RESPONSE | PEN TESTING
VCISO | WEB3 & BLOCKCHAIN | MANAGED SIEM
HELPDESK | IDENTITY MANAGEMENT
DISINFO MANAGEMENT



REAL-TIME THREAT
DETECTION



REAL-TIME THREAT
RESPONSE



PROTECT YOUR ENTIRE
NETWORK



PEN TESTING AND
VULNERABILITY SCANNING



REDUCE YOUR IT/SECURITY
WORKLOAD



AFFORDABLE
PRICING

FORTIFY24X7.COM | (800) 989-2647 | INFO@FORTIFY24X7.COM



PRODUCT REVIEW

SLNT E3 FARADAY BACKPACK

By Michael Bazzell

I confess I am a backpack junkie. I tend to purchase a few different bags every year and constantly chase the perfect bag for my travel possessions. I strive to take advantage of every inch and possess a bag with absolutely no wasted space. I have issues.

I recently picked up the SLNT E3 Faraday Backpack for some international travel, and put it through some brutal testing. I will offer the good and the bad here. SLNT is a sponsor of this issue, but I was not paid for this review. They do not even know that this review was written.

First, we should address the Faraday aspect. **The entire backpack is not a Faraday bag.** The backpack contains two pouches which have full Faraday protections (one for a laptop and one for a mobile devices), but any other area of the backpack is not fully protected from all signals. I am fine with this, as my underwear is not broadcasting any signals (hopefully). Let's focus on these pouches.

The mobile device pouch is big enough for a large phone. It has two nubs on the back which keep it secured into its slot in the front section of the bag. The laptop pouch held my 15" laptop without issues and has the same style of nubs for securing it in the back section of the bag. I thoroughly tested both Faraday bags and confirmed there was no signal leakage. Both have magnetic closures for discretion. The following image displays these nubs, with only one connected.



I am happy with the pouches, and are exactly as expected. These are the only areas of the bag which are fully

protected from all signal transmission. The main compartments have no protection, and should be used for non-transmitting items. I see a lot of people claiming that the entire bag is blocked, which is not true (and not as advertised).

My next favorite feature is the zippered pouch on the side of the backpack, at the very back where the pack meets the back. This section has RFID protection and can be used to store IDs, passports, etc. Since it is near the body, it would be more difficult for a criminal to get in unnoticed. When the pack is on my back, it is very difficult to see this pouch option, but I can easily access it to retrieve anything needed without opening the entire pack.

This pack includes a removable packing cube, which I eliminated at first. Since I rely solely on one bag when I travel, I have grown to appreciate this option. It allows me to stuff as much clothing as possible into this thin bag, knowing it will easily slide into place when full. It was much easier to remove

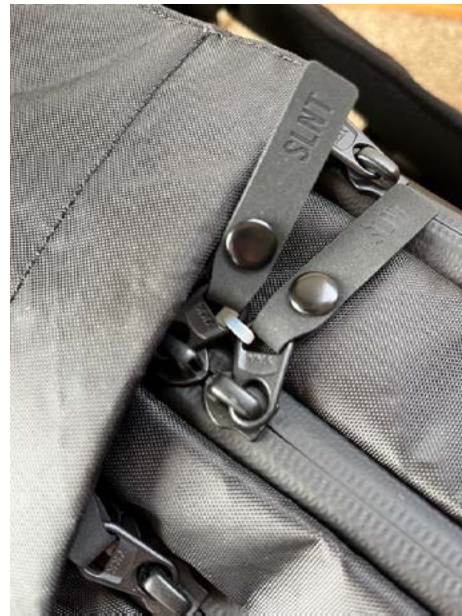
this packing cube and access my items than to dig from the top of a zippered backpack. The following images display the packing cube outside and inside of the bag. I was able to fit my entire clothing for the week in it, but I am a minimalist traveler.



There are over 15 pockets of various sizes, but everyone's needs will be unique here. I prefer to avoid small compartments in order to keep all of my items together. I hate opening ten pouches while trying to locate an item. Many of these pockets go unused during my travels.

The straps and handles are great. All are high quality and carrying the backpack vertically or horizontally from the handles was easy. The back straps held up well and offer customization. I wear my backpack high so I keep the straps tightened.

I was able to use small zip ties to lock the zippers in place during dangerous travel, as seen in the following images. However, when the zippers were tucked into the side pouch, one could still see them. I would have preferred a side pouch which was slightly higher in order to hide the zippers from view, and make them more difficult to access.



I liked the magnetic sternum snap for extra security from a snatch-and-grab. Fortunately, I was unable to test it. Overall, I was very happy with the bag, and at no time regretted bringing it as my only option. However, no bag is perfect.

The exterior material can sound a bit "crinkly". This is not a big deal, but if you are used to a silent cloth-type bag, you may hear the difference. However, this will offer better moisture protection than anything silent.

Next, the zippers would slightly catch on occasion, requiring me to pull them back and then forward again. This hesitation decreased over time, and may have just been an issue of needing broken in. This only occurred because the zippers are protected by material extremely tight to the zipper. You can see this in the previous images. You are not seeing the zipper teeth, that is the protective barrier from natural elements. Therefore, expect tight zippers, which can be a good thing.

Finally, this bag is not cheap at \$330. However, it seems that all backpacks (and everything else) just keep getting more expensive. Considering this comes with two SLNT Faraday bags, one of which is extra-large, I believe this is a fair deal.

The bag held up well throughout all travels and did not appear "flashy". I will continue to use it on longer trips. The muted dark colors and barely-visible logo allowed me to blend in well. SLNT offers readers a discount on all products at <https://slnt.com/discount/IntelTechniques>. Again, I was not paid (or even asked) to write this review. ■



DIGITALLY DISAPPEAR.

Protect all of your devices with
SLNT® signal blocking Faraday
bags. Disrupt the grid.

SLNT®

SLNT

INSTANTLY BLOCK



CELLULAR



WIFI



BLUETOOTH



GPS



EMF



KEY FOB



RFID/NFC



SAT/NAV



EMP/HEMP



SOLAR FLARE



SIGNAL

SLNT.COM // @GOSLNT



Image: Deepak Gautam

WIRELESS SECURITY: ASSESSING AND MINIMIZING YOUR RADIO FREQUENCY TRAIL

By Reginald

You leave a trail when you walk around town... well, maybe not you, but most definitely the gal or guy next to you does. For the last few millions of years, that would mean a predator could track you. That neighbouring tribe who covets your access to fresh water or your lush hunting grounds will find your spoor (the signs you leave whilst bundu bashing through the veld) and track you down, eventually finding their prey and perpetuating that age-old tribal turf war.

Today, the chances of that are mostly rare--mostly--but we still leave a trail on concrete and steel. Your spoor is invisible to the traditional tracker, but gifts the sophisticated hunter so much more to work with. Your predators know your every move, how long you stay or go, what you are using, how you use it, what you're looking at, what

you're hearing, and to whom you're talking about it. Let's take a moment and address what we like to call your RF trail--all those radio signals you bleed just by doing the things in which a modern human likes to do.

Each section considers how to anti-track (eliminate the signals) and counter-track (change the signal to throw trackers off the trail). Please be advised that we are surveying a typical everyday-carry scenario and technology knowledge level. Those of you who are more advanced with wireless technology may have some notes. Please share them for the benefit of all.

An individual's RF trail, in networking terms the Personal Area Network (PAN), usually starts with mobile phones. Peripheral devices like headphones, fitness trackers, smart watches, and other gadgets use a mobile phone as the master device to control and

coordinate a PAN. To achieve this, a typical mobile phone has five major radio chains; a radio chain is the path a signal follows to or from a device to enable communications--we're looking at a power source, processor, network interface controller (NIC), antenna, and whatever is needed in between:

1. Cellular Network for voice and Short Message Service (SMS)
2. 3/4/5G Data Network for mobile data (your LTE and 5G)
3. 802.11 Wi-Fi
4. 802.15 Bluetooth, typically Bluetooth Low Energy, or BLE
5. Near Field Communication (NFC), and other sub-gigahertz RF technologies, like RFID

Cellular is, in fact, a whole separate operating system, and can support broader operations, like satellite

phones. We'll focus on the more typical use cases. Bear in mind that phones aren't the only game in town. Health-related devices like pacemakers, insulin pumps, blood-sugar sensors, and the like also give off a RF signature. It must be made clear that your health and well-being are more important than elite RF security practices, and let's walk into this with that in mind.

Cellular Service, LTE, and 5G

Your 3G, 4G LTE, and 5G phones use a wide swath of frequencies to operate. LTE uses ranges between 850 MHz and 2 GHz, while 5G has low, middle, and upper bands. Using the U.S. as our sample, the majority of 5G runs between 2.4 GHz and 4 GHz, and newer implementations above 24 GHz, where speed and data capacity are way above average. In rural areas where distance range and penetration of vegetation is more important, low band 5G, at or below 1 GHz, is best, since lower frequencies trade data speed and throughput for stronger signals over long distances. Deeper diving into mobile cellular is out of the focus here, but expect more RF spectrum allocation to 5G development and upcoming 6G networks in the coming years.

The RF trail left by cellular is obvious at times--cell towers require every device in their footprint register for service. These towers collect and process multiple device identifiers, mostly to determine how to provide voice and data channels, and if they are current on their bill. Quality of service demands require geolocation, which towers can do via triangulation by three or more towers. If there are only two, or just one tower, the locations of devices are calculated based on signal-distance traveled estimates--a decent but highly watered-down analogy is sonar. In specific cases where smaller cells are installed, like pico- or femto-cells, the cellular range is more limited, and any device registered can be placed inside a much more manageable area.

At large public events where additional cellular coverage is needed to augment the existing towers,

technology like this is used. The information is maintained by telco operators, and available for use based on your service contract. Breaches, leaks, subpoenas, and commercial sales are just a few methods these data get shared. For typical mobile phone service customers, there's no way to deny geolocation on a cellular network and still enjoy the service without some hills to climb. Speaking of portable cellular tech, it's worth mentioning Stingrays--the infamous cell phone collectors associated with law enforcement and intelligence services. These act like a cell tower but offer no cellular services, collecting various device identifiers while discerning location, among other capabilities.

Cell towers are not the only collection points. Smart phones share location and activity through the device protocol stack, typically at layers deeper than a user can control. Services like electric scooter and bike rentals rely on apps to administer the rental contract. These apps operate through the cellular network, and won't budge unless able to access the mobile device's location. The app then reports your entire route. Back-end servers correlate that route, and the time it was taken, with anyone else sharing that route at the same time.

Likely these data are sold to other companies and agencies for additional profit, who then also know yours and your companion's routes, stops, and mobile device data. When breached or leaked, these data present a severe pattern of life and travel risk. Here we have the age-old balance between risk and convenience. The good news is that we have some easy ways to anti-track it, but we give up 100% of its communications functionality. The less good news is that we need to do some work to enjoy cell service but retain some privacy and security.

Anti-track:

- Use Airplane Mode if not needing to make or receive calls and SMS--other radio chains in your phone can still operate in this mode

- Faraday bags will block all incoming and outgoing RF
- Powering off disables the radio chains
- Relying solely on Voice over IP and chat using end-to-end encrypted apps--do this over Wi-Fi, including hotspots, and refrain from installing a SIM card
- Any combination of these

Counter-track:

- Mobile hotspots will register device IDs other than those associated with the hotspot--keep the mobile phone off of the cellular network
- Anonymous or pseudonymous phone and service purchases, like pay-as-you-go plans that do not require adherence to Know Your Customer policies

Older Androids used to allow connections to mobile data while in Airplane mode, but this seems to have been restricted as of Android 12.

Wi-Fi

Wi-Fi is a powerful and widely used technology, but suffers from constant security and privacy challenges. Wi-Fi pumps out up to 0.1 watt at both the 2.4 GHz and 5 GHz ranges. Newer 802.11ax technology can utilize the 6 GHz band as well, but this isn't widely adopted yet. If you see marketing for Wi-Fi 6E, this is the "extended" Wi-Fi 6 offering 6 GHz band service. As a comparatively open and unsaturated section of the RF spectrum, 6 GHz Wi-Fi is very attractive and worth the cost to implement; expect it to be used routinely with the other two bands in the near future when 5G cellular and Wi-Fi 6 steadily integrate their authentication and security features.

For now, the advantage is with the predators. Our observations prove that most mobile phone users pay little attention to their Wi-Fi settings. There is no incentive to turn Wi-Fi off throughout our daily routines. Turning it off when we leave a trusted wireless network,

and on again when returning is an extra, and perceptively unnecessary step. The challenge lies with Wi-Fi's very chatty nature--your device is constantly asking the airspace around it if those networks you have saved are nearby. It wants to connect using the saved password and provide the user a smooth and high-quality experience. This happens as long as the Wi-Fi is active, even if the device is already connected to a saved network. A predator can collect these requests your Wi-Fi radio is making, and see your phone's, tablet's, or computer's name, MAC address, name of the networks for which it is searching (service set identifiers--SSID), and a host of other useful data. Using tools like Wigle, a repository of crowd-sourced wireless network signals (<https://www.wigle.net/>), anyone can search for networks by SSID and/or MAC address. A predator that sees the ones your device is yelling for can find them, plot them, and develop a pattern of travel and usage. If that isn't important to you, then consider that your Wi-Fi's chattiness spends a lot of battery power too, and for those who cannot regularly charge devices, this is crucial.

Of great concern are Wi-Fi-based malware attacks. Devices using open wireless hotspots are placing a lot of trust in that network, with no knowledge of who else is using it. Without getting into specific Wi-Fi hacking, attackers use numerous methods to exploit users on public networks. A very popular one is a rogue access point, often pretending to be a legitimate one, waiting for devices to mistakenly associate with it. That attacker now has full view of those victims' activity. If you are indeed a target for a digital predator, connections to public networks, especially open Wi-Fi, open your attack surface up more than most other cases. Tread with extreme caution, if at all, using public Wi-Fi.

Anti-track:

- Be disciplined about turning Wi-Fi off when not in use
- Disable auto-connection to open and unsecured Wi-Fi

- Delete saved networks; keep the SSID and password saved somewhere else for future use--secure notes apps and password managers are a great option for same-device storage
- Refrain from public Wi-Fi, especially networks with no authentication--in fact, experts on the topic would advise avoiding public Wi-Fi altogether and relying solely on mobile data

Counter-track:

- Newer Android devices allow MAC randomization on wireless networks
- Wi-Fi antenna dongles, for USB typically, will display that dongle's MAC address, obfuscating your device's built-in 802.11 MAC address
- Mobile hotspots and travel routers perform the same service, but with much more functionality and accommodate multiple devices--travel routers usually allow MAC cloning...

MAC address cloning is exactly what it sounds like--you can have your travel router pretend to be another device by altering its MAC address to look like the other device's. This is how some travelers negotiate public Wi-Fi authentication and splash pages. For example, if you know of a device that is associated with a Wi-Fi network, thus its MAC address is white-listed, then you can also be associated with that network if you display the white-listed device's MAC address. That is a somewhat simplistic description of the technique, but it works. Next time you are at a hotel and your travel router cannot associate with the Wi-Fi due to a splash page, use that Wi-Fi antenna dongle on your laptop to log in, then clone the dongle's MAC address to your travel router. No guarantees, of course, but it tends to allow your router to associate as if it were the original antenna dongle. Bear in mind that many hotels reset associated device lists daily, so you may need to perform this technique multiple times during a lengthy hotel stay.

Bluetooth, NFC, and other short-range PAN technologies

Bluetooth comes in several flavours, but the most popular is Bluetooth Low Energy (BLE). It operates in the same RF space as 2.4 GHz Wi-Fi, though its design tends to keep the two protocols from interfering with one another in all but the most specific cases. Bluetooth uses an antenna with a MAC address, just like every other NIC in your device, making it unique and separate from the Wi-Fi signature. The BLE explosion of the past decade or so left the world with myriad options for PAN connections. Headphones, watches, various monitors for health and movement, portable speakers, VR headsets, and many others stay with us wherever we go, usually linked to our mobile phones acting as the controller and orchestrator of the personal BLE ecosystem. It gets very noisy when so many devices are paired and communicating, but BLE has a working range of 80 - 100 meters on a good day in a flat, open parking lot. Typical ranges are more like 60 - 75 meters under most conditions, and that range decreases as one passes through denser media. Near Field Communication (NFC) is similar enough that the typical user wouldn't distinguish it from BLE aside from the services they offer. NFC has considerably less range (typically 1 meter or less) and acts more efficiently with power and data. An NFC function requires no pairing or device-wise negotiation, which is why you can use apps like Apple Pay or tap a NFC-equipped credit card to make a payment, and not have to push any buttons or wait for a connection. Operating at a mere 13.56 MHz, it doesn't support much data transfer capacity, and considering its uses, doesn't need it.

A predator looking to exploit your BLE PAN would need to be in that range to detect the signal, and from there needs to discern your devices from everyone else's. That is assuming you alone are the target. A malicious actor may choose to attack all BLE devices within range of their attack equipment. You'll experience devices being unpaired until you get some distance from the attack, resulting in some work to reconnect.

NFC has more resilience to these sorts of denial-of-service attacks, since anything disrupting it would have to be so close as to be noticed. The average user's NFC profile has many built-in fallbacks as well, like inserting your card's chip or just paying cash instead of using your phone. NFC used to be used for features like Android Beam to share data directly between devices. Competition from Apple's AirDrop and Google's Nearby Share, which use Wi-Fi and Bluetooth, have since driven many NFC-based data sharing apps out of the picture.

If you are the target of a wireless bloodhound, then things change a little. Our wireless predators need not just be malicious actors; your local department store is becoming our worst wireless enemy these days. Places like Walmart and Target, for instance, use BLE devices placed strategically within their stores to detect and record BLE signals of customers' devices. If you happen to have that store's app installed on your phone, and your Bluetooth antenna is powered on, be prepared to enjoy opportunistically timed coupons that offer a discount on that item you happen to be eying at that very moment. BLE technologies like iBeacons--Apple's indoor positioning and analysis technology--can locate a mobile phone (not just iPhones) down to the product's placement on a shelf in an aisle, cross-reference the device's information as passed by the installed app, and send push notifications at will. The money-saving implications notwithstanding, you're being tracked in real time for the sake of advertising and increased revenue. The next time your favourite department store suffers a data breach, all of that becomes likely seed information for some convincing email or text message fraud. Be wary of your Bluetooth signal, but let this be a quick nudge about store apps too.

Anti-track:

- Be disciplined about turning Bluetooth off when not in use; NFC and services like Nearby Share can be turned off as well

- Delete saved Bluetooth paired devices you no longer use--like Wi-Fi, that list can give some of your PAN profile away
- Credit card sleeves designed to block RF will help to block your cards from throwing their NFC data off to the world unless you deliberately remove and use the card
- RF-blocking wallets and bags, like Faraday bags designed for phones and computers, provide the same function
- Using good old 3.5 mm headphone jacks and skipping Bluetooth use altogether; this works great for your car, and highly recommended for rental cars--you share audio only and no data

Counter-track:

Techniques like changing Bluetooth device MAC addresses takes some time and education that a typical user may not enjoy. Those with higher threat profiles may look to carrying multiples of the same device in order to increase collection entropy, but that's an expensive tactic, and rather puzzling when more traditional and wired solutions are available. Those who are more technical and intrepid with mini-computing and radio technology can try to build BLE, NFC, and RFID spoofers and test them out. Please share your results.

Some Best Practices

More and more public areas are being equipped with RF signal detection capabilities, and protocols like Wi-Fi and Bluetooth, which beacon unique MAC addresses and device names, among other items, will place your device at that location at that time. Notice that it places your device, not you. It's a distinction that some may not appreciate as much as those who know how to clone and spoof MAC addresses. With the advent of Smart City/Safe City developments, more and more of our public places are designed ground-up for wireless collection. The

following are common habits adopted to minimize the amount of collectable RF from our PANs, without getting too extreme:

- Strict adherence to toggling Wi-Fi and mobile data off when not in use--again, this is a battery saver if nothing else
- 3.5 mm jack cords in lieu of BLE connections to speakers, headphones, and cars--great option for rental cars where a data connection carries risk
- Related to that, adopt a stand-alone navigation solution for your vehicle, instead of using your phone's GPS; bring it with you on trips if renting a car
- Cutting the fitness app cord if you can--some individuals require these or other essential medical devices and their requisite apps for life-saving purposes, and that overturns any suggested best practice
- Leaving the phone in the car when visiting the grocery and department stores, the mall, and government buildings (this makes you effectively invisible in these places)
- Leaving smart watches and glasses out of your PAN altogether--you sacrifice some convenience, but this tech is outrunning the security measures to protect it
- Using RF-blocking card sleeves, wallets, and bags for everyday carry

These are just some of the basics to cut down your body's RF emissions and throw predators off your trail. Wireless is a vast and exciting world, but that sword has two edges.

You still leave a trail when you walk around town, but you're probably doing a little better. The myriad antennas in your phone, connected to their own radio chains, and running off of multiple ARM chips, work hard to make sure you get the most out of your device, and it works how you want whenever you need it. As you become more

judicious with powering those radios only when needed, they now work hard for you and on your more secure terms. Let's now dive a little deeper and expand your emissions control for even more anti-tracking, exploring our collection of RF-capable cards and our vehicles. Before we step off, some of these tactics and techniques are not more advanced or complicated than taming your mobile devices, but they are things that we've seen overlooked by most people. Others, though, especially when confronting the newest connected vehicles, present daunting anti-tracking challenges. For now, if we can't stop it, let's at least be aware of it. Praemonitus praemunitus!

Out in Town

Stepping away from phones for a bit, let's explore other RF sources that track with your body's movements. Bank cards, NFC-capable ID cards, entry badges, and other sub-GHz emitting wallet-sized items typically inhabit our pockets and bags. Most of them are passive RF technologies, meaning they only respond to an active RF source, like the touchless payment pads on gas pumps or readers at access control gates. Other active RF sources can be placed just about anywhere, and may engage the passive RF tech you carry, intentionally or otherwise, if you come into close enough proximity to them. Protection against this is low-cost and requires nothing more than inserting these cards into RF blocking sleeves or a RF blocking pouch.

To drive the point home, a sample attack against an unsuspecting credit card in your back pockets can go as follows: an attacker nearby will walk very close to you, if able, collecting any RF emissions at credit card NFC frequencies; this is a dynamic form of skimming, but collects much less. The attacker succeeds if they gathered your name and credit card information. The good news is that the CVV number isn't included in the NFC transaction, nor are essential keys to enable transactions, but the privacy damage is done now that your name and CC number, transaction counter, and expiration date are known. A more advanced

version of this has a second attacker receiving what the first one collects in real time over a wireless relay. The second attacker now uses their device as a proxy for the victim card at a point-of-sale station. Yes, this happens; look up an Android app called NFCProxy. We recommend RF blocking sleeves.

At the Gates

More danger appears when RF readers are powerful enough to overcome the limitations of everyday usage, and are snooping nearby. The gas pump touchless payment sensor needs your credit card to be within 2 centimeters in most cases to correctly operate. A radio receiver tuned to that active RF reader's operating frequency, using a focused antenna and enough power, can capture the transaction between your RFID card and the gas pump. The same operation can capture interactions between access control systems like HID cards or tags and reader panels.

Very briefly, access control card readers use several protocols, the Wiegand protocol being one of the more widely used, to communicate with user cards. Many of them do not provide encryption during these transactions, and thus will give details away to ambitious snoopers, like card IDs, vendor IDs, and other tidbits which could be attributed to the facility, and at times, the card or tag owner. Newer protocols are adding encryption to these operations now. To the card user, there is no way to tell. Realistically, the threat is to the facility and not the individual. Reading your RFID transactions can possibly let an attacker clone the card or tag, or create one that can also gain entry. These threats become serious if the system is for a home or other secure space, and passes identifying information.

How can we defend against this? Without encryption, the best defence we have is our own human body. Low power RF operations at the sub-GHz level often are dampened by bodies. At the gas pump, HID panel, and contactless turnstile, hold the RFID tag or card close to your chest or hips while

in use. Act like you're entering your ATM card pin with a crowd of onlookers shoulder surfing. A second tactic is using that RF blocking wallet, pouch, or bag as a shield during the RFID transaction. Close the distance as much as possible to minimize the space any RF has to travel. Please don't smother the RF emitting devices, as that will deny the communication. No, these are not very exciting defences, and are not 100% effective either, but it is what we have until adoption of encryption in RFID access control systems is more widespread. We encourage anyone who has better expertise and solutions to please follow up here.

On the Road

We touched on using audio cabling to connect mobile devices to a vehicle's entertainment center, and not Bluetooth Low Energy (BLE). Provided the phone's BLE radio is off, this tactic will disentangle your device signature from the vehicle. If you have the ability to disable the vehicle's Bluetooth radio as well, consider it. If not, check if you can change the Bluetooth pairing name to something which doesn't identify you or the vehicle, if it is not already. We can dive a bit deeper into vehicle RF emissions now.

Using a mobile phone to enable a car's network connection is commonplace, especially for GPS navigation and hands-free phone usage, either via BLE or a physical USB cable connection. Still focusing on RF emissions control, a USB connection is preferred over a wireless one to eliminate the BLE signal, but we're left still with cellular and mobile data connections. If the vehicle has the right chipsets and computers on board, that USB cable shares the mobile network with the vehicle too. Very common apps like Android Auto and Apple's CarPlay make this sort of connection sharing with cars quite easy.

Modern vehicles feature several levels of connectivity, intended for user quality of service and experience. Privacy4Cars, a technology initiative focused on increasing data privacy and compliance in the automotive industry (privacy4cars.com), published their

“Five Levels of Vehicle Connectivity”. The lowest, level 0, allows no wireless capability, while the highest, level 5, contains natively installed wireless connectivity through embedded network controllers. Most drivers have a level 2 or 3 vehicle, which, according to Privacy4Cars, offer indirect or direct connectivity through end user mobile connections, respectively.

In this case, it is best to be aware of your car’s capabilities, and be mindful of what is shared when you connect your phone. Unless you are technically and electronically savvy enough to disable your vehicle’s built-in SIM or other radio chains without “bricking” it, items like location, driver and occupant behaviour, telematics, and application usage are stored locally by the vehicle and often shared with third parties. We recommend segregation; limit or stop phone connections altogether to deny your car any network access. If you choose to use your phone for navigation, refrain from pairing it with the vehicle’s “infotainment” system. Of course, this may deprive you of a bigger display option, but as previously suggested, consider a stand-alone GPS unit to curb your phone’s RF emissions, or the potential to connect your car.

Let’s quickly survey some other often overlooked RF sources. If you possess a toll payment device, like E-ZPass for certain U.S. interstates, be aware that these transmit your vehicle and toll payment registration information to any sensor equipped to read it, not just toll collection points. The extracted data reveal your travel to very detailed degrees. The security of these wireless transactions varies among the services, but are generally weak if present at all. We recommend storing them in a RF blocking container until needed, or leaving them at home if not used for regular travel.

Ham radio operators install and use mobile transceivers, ranging from simple GMRS plug-and-play boxes to highly sophisticated digital-ready HF or multi-band rigs. These radios are designed with service and connectivity

in mind, but every ham should know that most RF regulating bodies worldwide prohibit encryption, and your transmissions are susceptible to direction finding and triangulation. If this is a large part of your threat profile, consider reviewing your operations security (OPSEC) whilst transmitting to minimize any sensitive information, and factor for vehicle speed, direction, surrounding terrain, and length of transmission to increase your comms security posture. This is possibly a whole article in itself.

Don’t forget built-in services like OnStar, Verizon Hum, SiriusXM, and other premium wireless vehicle services. Take stock of their features and carefully determine if you truly need them, and if those needs outweigh the RF signature giving your vehicle away on the road. Our recommendation is a no-service posture for numerous reasons—cost savings, decreased distractions, independence from crutch emergency services (potentially fraught with false positives), and maximized control of your car’s media through devices you own and operate on your terms.

Smart Cities and Cars

As the automobile industry evolves, newer vehicles will gain more networking capabilities. Certain countries are implementing new Wi-Fi and cellular standards for intelligent transportation systems, including vehicle-to-everything (V2X) technology. Very broadly, it will enable capable vehicles to communicate with transportation infrastructure networks over 5G cellular and Wi-Fi in the 5.9 GHz and 60 GHz bands. The data proposed for collection and dissemination are collision warnings, lane change and blind spot warnings, emergency vehicle approaches, roadwork warnings, and several others. One supported industry is autonomous driving, though inter-vehicle and other V2X modes can offer safety benefits right now. The tradeoff is, of course, the multitudes of data collection with potentially weak, if any, anonymisation.

Those hazards notwithstanding, Wireless Access in Vehicular Environments (WAVE) technology is inherently insecure in its current form. The two biggest culprits are jamming of the RF medium and lack of encryption due to latency and delay concerns; it takes time to encrypt and decrypt packets which vehicles traveling at high speeds don’t have. One can imagine the exploitation possibilities. More and more cities globally are adopting this sort of “Smart” technology and evolving towards aptly named “Smart Cities”. The evolution is outpacing the security, and leaving privacy concerns in the dust.

The short answer is that we likely won’t have any real methods to curb these communications. It’s best now to be aware of these potential technologies. If that is a large part of your threat profile, start researching vehicle purchases by means not associated with your identity. This topic is admittedly complicated and outside our current scope, but covered in great detail, among myriad other topics, in Bazzell’s *Extreme Privacy*, Fourth Edition.

A Word from the Red Team

As we tour the various RF we bleed, and attempt to control it, please resist the urge to shun radio technology as the enemy. It is not. RF technology is a vast and fascinating realm, and whether used for good or malice, is simply a tool for a job. Learn about it by exploring how hackers deconstruct transmissions, how ham radio operators enjoy their craft, or how developers create new ways for people to connect. There are few barriers to entry for radio as a hobby. An inexpensive UHF-capable hand-held radio is enough to start hearing others—your local fast-food restaurant likely uses a Family Radio Service (FRS) channel to confirm drive-thru orders. Why not find it while waiting in line and make sure they got yours right? From there, the wireless world is yours. ■



Image: Koby Kelsey

HOW YOUR APPLE ACCOUNT CAN BE COMPROMISED WITH JUST YOUR UNLOCK PIN

By CL

Disclaimer: This article is accurate at time of writing but will be updated after Apple finalizes and releases iOS 17.3 with a stolen device protection feature.

I recently had a family member get robbed at gun point and after talking to her there were a lot of lessons to share. Name changed for anonymity.

This was a winter day around 3-4 PM and Gloria pulled over in a neighborhood to make a call. She had

a lot on her mind and wasn't paying as much attention to her surroundings as she normally would. After a few minutes a car pulled up on her left. A young man about 15-16 years of age got out and pointed a gun at Gloria. Gloria's first instinct was to put the car in drive and get away. The young man said: "You don't want to do that. I'll blow your head off." Gloria put the car in park and then another man came up on the opposite side of the car to open the door and one more man on the driver side pulled her out of the car. They quickly obtained her keys and phone and held a gun to her head and

demanded the iPhone screen unlock PIN. Gloria tried protesting saying that the phone was already unlocked from her phone call and on the home screen but the thieves were undeterred and asked again: "What's the password to your phone?." Gloria told them the screen unlock code. They didn't ask her for her iCloud password and only asked her twice for her iPhone password. They got in her car and left with both vehicles. The whole event was over in less than 3 minutes.

As Gloria tried to secure her account, she discovered they quickly reset her

iCloud password and had transferred money out of her Cashapp.

There is a lot to unpack and learn from Gloria's experience and how to limit the damage from going any further. I am not writing to rip on Apple but only to highlight some less than obvious holes in their security decisions so you can be more prepared if something like this happens to you.

To summarize up front: Apple boiled the entire security of an Apple account down to a trusted device and a screen unlock PIN/Password with no way to secure the Apple account any further. I will explain below.

Apple has taken a stance of convenience over security that works against the victim in forced scenarios with no way to protect your account from someone who has a user's iPhone and screen unlock PIN/Password. If you reference Apple's Apple ID password reset document it explains that all you need is a trusted Apple device to reset your password. Since a stolen iPhone with a screen unlock PIN/Password is a trusted device your Apple account is effectively completely compromised. All your documents, contacts, calendars, photos, iCloud passwords, backups and everything else stored in iCloud is completely available to the thief all because of your screen unlock PIN/Password. Your iPhone can even be used to factory reset all your Apple devices making account recovery even harder and the data loss damage potential extreme. While Apple flaunts Apple ID security for protecting its users from unauthorized access they take measures hostile to their own users if a user's device is compromised. Advanced Data Protection also won't help in this scenario and there is no way to secure data you have in iCloud if your trusted Apple device is compromised. Even Apple's recent support of security keys like a YubiKey won't help you because your phone is still a trusted device which has the same level of access as the security key (although if a thief doesn't know to disable the keys you may be able to regain control of the Apple account).

Additionally, if you are a part of a Family Sharing account then this trusted device could be used to reset any other Family Shared device or the other way around. If this type of theft happens to your mom and you share a Family or Premier Apple One subscription then the thief can use Find My on your mom's phone to reset all of your Apple devices. They won't have immediate access to your account, but some damage and data loss will be done. Depending on the circumstances it is even possible for your Apple account to be compromised if the person whose phone was stolen is selected as a Recovery Contact for your Apple account.

Below are some ways to lessen the impact of this situation if it happens to you and are not limited to Apple users (but some mitigation examples will be Apple focused). Some may not be possible for you, and some may just be points to consider for protecting your own information. This situation is best to avoid completely by being aware of your surroundings, not looking like a target, and avoiding certain areas but it can still happen to anyone and the mitigation of loss by preparation is what I will focus on.

1.) Consider spreading your eggs into other baskets that have better protections. Using an iPhone isn't insecure and while I would consider these devices some of the most secure, they betray you in forced unlock scenarios. It would be wise for some sensitive apps to make sure they have secondary lock screens. There are cloud storage apps that when you open the app you are forced to enter a PIN or password to unlock. If you make this PIN separate from your device unlock PIN then it is unlikely the thieves will stick around long enough to go through all your apps and ask for individual PINs. Some apps allow you to unlock with a fingerprint or FaceID. This can be a convenience option for unlocking but it is very important you test that it falls back to prompting for a separate PIN or password if a new or second face or fingerprint is added as not all apps do this (or just let you use the device PIN instead of a separate second PIN).

For other types of data like passwords consider something like Bitwarden instead of iCloud Keychain. Bitwarden will prompt for your master password if a new biometric credential is added so you gain both security and convenience from switching password managers. In order to assess the damage losing your unlocked phone may have just go through your apps and see which ones are accessible without putting in a PIN or password.

2.) Prepare for loss of your phone without recovery. It is almost certain if your phone is lost in this type of theft that you will never get it back. The only option to mitigate the thief from resetting your remaining Apple devices is by turning off Find My access for your devices. If you are worried about losing your phone without Find My turned on, your phone may still be able to ring if you use Do Not Disturb and call your phone twice to bypass the Do Not Disturb silencing. You will also need to either separate your accounts from family sharing or have your family members remove their own devices individually from the Find My network to limit the possibility of their devices being reset. If you must leave your devices on Find My I would at least recommend turning off Find My for devices you are far less likely to lose like a Mac desktop, Laptop, iPad or any other device that doesn't leave your home. Home invasion is always possible, but these devices should be protected by the screen unlock PIN/Password and then the other devices in the family accounts are not at risk.

3.) Reduce apps and accounts you have on your mobile devices. We all know your magic rectangle can do just about anything, but do you need it to? Do you need a mobile payment app like PayPal, Cashapp, cryptocurrency or some other payment app or service on your phone? It sure is convenient but for this scenario it will cause you lots of headaches. If you need to use PayPal, use it at home on your computer. Credit and debit cards still work just fine and afford you protections for your money that cash and cash equivalent apps may not afford.

4.) Separate your car key from your home or other keys. Don't keep your wallet and phone in a case together. This is actually similar to recommendation number 2 but for physical things. By removing your car key from your home or work keys and your phone and wallet separate you at least create the possibility that only one will be lost. A thief isn't going to wait around for you to undo your work or home keys from your ring that has your car key. For RFID keys take a look into RFID blocking pouches for keeping keyless fobs in during storage at home or a hotel (as this can prevent spoofing theft). For the loyal fans of real physical car keys this helps reduce strain on your lock cylinder and can help your ignition last longer. It may also be worth your time to look at how much stuff is in your wallet and what can be left at home.

5.) Reduce the data of your home, work or other place you frequent from your phone or car navigation apps and glove box. This one might not be as obvious but applies outside of forced phone theft scenarios. I bought a car

a few years ago and it still had the previous owners home address saved in the navigation unit. If the dealership I bought it from didn't wipe the information from the navigation unit, then you can be sure they didn't wipe the Homelink garage door opener built into the mirror. If you got rid of a car without wiping the garage door opener from the car you can wipe all previous saved garage door opener remotes from the opener memory (but you will need to re-pair your current garage door openers and keypads). If you print out your insurance information it may be worth it to keep that information in your pocket or in a hidden place in your car in case of car theft so that it is less likely a thief can find your address and target your home after they steal your car.

6.) Memorize a phone number of someone important to call when you need help. If you don't know the phone number of a friend or family member to call if this situation happens to you then you should memorize it. You won't have your phone book to fall back on

right away and you will likely need a ride home and to start making phone calls to lock accounts and recover.

7.) Make a document for phone numbers to contact in case of wallet loss. Find out customer service numbers for if you lose your credit, debit or other cards to lock your accounts and keep it at home or with your important contact above.

8.) Use disappearing messages to get rid of old messages you don't need. We are all different, but I can say most messages I send my friends don't need to exist after a week. I wouldn't want my sensitive chats published and by simply making sure that I only have very recent messages then the damage can be limited.

If you do find yourself in this or a similar scenario it is unfortunate, and I send my condolences. I hope the above recommendations help you to plan for these losses to make mitigation and recovery efforts easier. ■




UNCHARTERED

**DUE DILIGENCE | RISK ASSESSMENT |
SOCIAL MEDIA MONITORING | SUPPLY CHAIN | DARK WEB |
BRAND REPUTATION MANAGEMENT**

UNCHARTERED.INFO

GETTING READY FOR A POST-QUANTUM WORLD

TUTA IS ABOUT TO LAUNCH POST-QUANTUM SECURE ENCRYPTION FOR EMAILS

Sponsored Message

Quantum computers will introduce unique computing capabilities and with this give rise to completely new tools and services, revolutionizing how we use the web today. But at the same time, this unseen-of computational innovation threatens the security backbone of the internet: namely asymmetric encryption. The looming threat of quantum computers on traditional cryptographic systems prompts the need for post-quantum encryption algorithms. This article explains how we at Tuta are updating our cryptography to secure email communication in the post-quantum era.

The advent of quantum computers, together with Shor's algorithm, threatens the foundations of conventional public-key cryptography, such as RSA and ECC, which is widely used to secure email communication. Thus, we at Tuta Mail have started a research project, called PQmail. Its first stage is about to be released to the general public. This project builds on the Signal protocol, known for its robust security features in instant messaging applications, to secure

emails with post-quantum secure end-to-end encryption.

You can read more on the adaptation of the Signal protocol for email in this paper: <https://eprint.iacr.org/2021/875>

Current State of Email Encryption

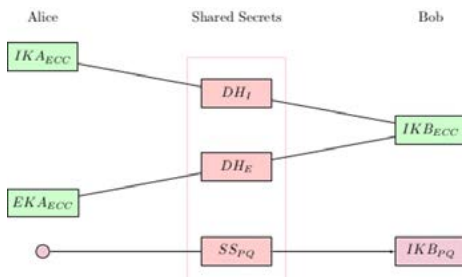
In spite of transport encryption with TLS, emails often traverse insecure networks and servers, making them susceptible to various attacks, including eavesdropping, man-in-the-middle attacks, and unauthorized access. All currently used email encryption methods, such as Pretty Good Privacy (PGP) and S/MIME, rely on asymmetric key algorithms that may be vulnerable to quantum attacks. Thus, a new approach is needed to securely encrypt emails in the post-quantum world. For this, a hybrid protocol – one that encrypts the emails with both traditional, proven algorithms, and with new, quantum-secure algorithms – is needed. Using a hybrid approach, in which an attacker would have to break both algorithms, is absolutely necessary as the new algorithms are not tested as much as the traditional ones and might include a vulnerability within the implementation that is not yet known.

Post-Quantum Security for Email Encryption

Signal has already launched post-quantum secure encryption for the initial key establishment of their chat app making it the first publicly available instant messaging application using a hybrid protocol to future-proof data against attacks from quantum computers. At Tuta we are eager to follow this great example and we are happy that we will soon release post-quantum encryption for emails to the public.

To become quantum-secure we had to update our cryptographic protocol to include post-quantum encryption algorithms, introducing a new key exchange mechanism, which we call «tuta-crypt». As explained, tuta-crypt is a hybrid KEM leveraging both well-proven classical algorithms and new quantum-secure algorithms to replace RSA. To achieve quantum-safety we use the recently NIST-standardized CRYSTALS-Kyber (1024) algorithm. In case it is broken - even though this is not deemed very likely by the research community - we also use a non-interactive Elliptic Curve Diffie-Hellman key exchange based on curve x25519.

The Kyber ciphertext, the public key and both shared secrets are used to derive a key with HKDF-SHA-256. This derived key is the root secret to symmetrically encrypt more session keys and ultimately also the email, subject line, and attachments. We instantiate symmetric encryption with AES-256 in CBC mode, authenticated with HMAC-SHA-256.



An overview over the public keys and how they are combined to compute shared secrets in tuta-crypt when Alice encrypts a message to Bob.

How Secure Is Tuta-Crypt?

Tuta-crypt is able to keep emails confidential both under the classical

and the quantum attacker model. The protocol also protects message integrity and ensures authenticity under the pre-quantum attacker model by including a shared secret only the designated sender could have computed. Furthermore, all symmetric encryption is authenticated, which means that even an active post-quantum adversary cannot tamper with it. At the same time, we manage to avoid signatures. Thus, the protocol also provides offline deniability, which means only the recipient is able to cryptographically link a message to its sender.

The tuta-crypt protocol is just the first step. We will still improve security when it comes to minimizing the impact of long-term key compromises. Therefore, future stages of our post-quantum encryption update aim to also provide perfect forward secrecy and post-compromise security by using our proposed quantum-safe version of Signal's Double Ratchet algorithm.

On Our Way To Quantum Resistance

The world is changing faster than ever, particularly in tech. With the upcoming rise of quantum computers we must make sure that our data stays safe in a post-quantum world. Our data must be encrypted with quantum-secure encryption already today. Otherwise, malicious actors can simply scoop up today's encrypted data that is shared over the web and store it for a later decryption. This attacker model is called «Harvest Now, Decrypt Later».

We admire the great work done by the Signal Foundation with their quantum-secure encryption of chat messages. Building on the Signal Protocol to achieve post-quantum security for email is a challenging task, but one that we at Tuta Mail are excited to take on. Our mission is that your data stays secure and private – now and in the future. ■

Don't Settle For Less: We're About To Launch Post-Quantum Encryption!

Secure Your
Emails,
Calendars
& Contacts
On All Platforms



Tutanota

Privacy. Done. Right.

tuta.com/unredacted





Image: Alexander Andrews

IT'S NOT ME, IT'S YOU: BREAKING UP WITH MY CELL PHONE NUMBER OF 21 YEARS

By Alec Harris

Any good investigator will tell you that the single best artifact to collect when building a targeting package against a subject is their cell phone number. I don't speak to data brokers (I'm sure the feeling is mutual) but I suspect they feel the same way about the value of cell phone numbers. More than your social security number, more than your name, address, IP address, ad tech ID, email address, browser fingerprint, or any of the other digital

identifiers, your phone number is you. Almost everything we sign up for asks for a phone number, and some, like Meta properties WhatsApp, Facebook, and Instagram require an actual cell phone number – burner VoIP lines be damned. Even services that technically don't require a cell phone number, like Gmail or Proton Mail, make it much easier to sign up if you provide one.

In 2002 cell phone adoption among US adults was 62%. Today adoption is 97% overall and 100% in the 18-49 age

group. This means that if you are 18-49 in the US and you don't have a cell phone, you are statistically nobody.

I was 18 when I got my first cell phone in 2000, right in the middle of the adoption curve. I remember being told I had a whopping 150 minutes a month and some amount of these things called "texts". I was in college at the time and the main problem I had with my Zack Morris-esque Nokia phone was that it didn't have "vibrate" so if, per chance, I was at a loud, uh, event, I couldn't hear

it. My solution was to put the phone in my front pocket facing out in hopes that someone looking at me would see it light up with an inbound call and let me know. I don't recall texting much, after all I had AOL Instant Messenger on my desktop in my dorm room, so I had the social written word covered. If you needed to know where I was, just check the away message. Stupidity ensued.

Prior to the undertaking described here, I had the same cell phone number since the 150 min Zack Morris phone. It was time for a change. Given how entwined we all are with our phone numbers, is it possible to make a privacy preserving shift to a new number without creating chaos? Yes.

After that 21-year run with my original phone number I decided it was time to see if I could add some rigor to my privacy practice and unwind my life from my long-held cell phone number. Honestly, I put it off for a long time. I thought it would be disruptive and time consuming. To some degree I was right, but it was not nearly as bad as I thought. Here's how you can do it too.

First and by far the most important thing in this whole process is that you should never, ever, release your cell phone number back into the wild. Imagine if someone got your cell phone number of 21 years randomly (or nefariously) assigned to them after you released it and used it as a vector to access your accounts or digitally impersonate you. Bad news. Got it? Good.

Now we can talk through process. You will want to port your old cell phone number to a VoIP provider. At my crafty day job, we can handle this on behalf of customers with our private number provisioning, but I wanted to go full DIY to show the mechanics. I spent several months looking into various VoIP providers. I was not impressed. Most have horrible security. Part of my vetting was to actually sign up for an account then attempt to change access to the account to see how easily it

could be done. In all but one case I was able to engineer account access with a phone call and information technically available through open-source. I say technically because some of it, like credit card numbers, might have to come from breach data, but it's still out there on most of us. VoIP services with a reasonable level of security tend to be geared for b2b sales. Practically, this means that single user accounts are at the most expensive rate. Expect to pay as much for VoIP as you would for a cheap cell phone plan. The cheapest option is Google Voice but not only can I not recommend it, I'll never forgive you if you use it. Admittedly some of my good privacy friends use Google Voice, it's just that I have a separate personal initiative to completely de-Google my life. More on that in a different article. Please get in touch if you want to know which VoIP service I selected. I consider it poor OPSEC to publish the provider so I won't list it here.

Once you've identified your intended VoIP service the next step is to pivot back to your SIM card. If you don't have a dual SIM enabled phone, I would recommend one for this project. iPhones starting with the XR model through the current line all have hard SIM + eSIM dual capacity. Before you port your current SIM to VoIP, add your new line as an eSIM. You will have two cell phone lines for part of this process. It is possible to skip the overlapping SIMs step, but the process is more forgiving if you opt in.

In selecting your new phone number & carrier there are a variety of things to consider including

Carrier Security, Area Code, Pattern of Life, and Payment.

Carrier Security

The three main carriers in the US are Verizon, AT&T, & T-Mobile (Sprint). None of them have sufficient security at the retail level. SIM swaps remain prevalent because of lax mechanical controls around subscriber account provisioning compounded with a very

large pool of carrier employees who can manage subscriber accounts. Between all the carrier employees in their call centers and the retail employees at stores, the social engineering target set for an adversary trying to co-opt access to your SIM card is too large to ever be considered fully mitigated.

I decided to get my number from a privacy-loving Mobile Virtual Network Operator (MVNO) that I know well and use regularly for day job projects. Feel free to contact me if you want to learn more but the gist is that my cell phone numbers are considered "carrier-hidden". It means that they are strictly managed outside of the main carrier retail databases. If I tried to go to a Verizon or AT&T store to get help with my number, they would not be able to look it up. This is an exotic offering, but the level of SIM card security provided is the best I've ever seen.

Area Code

Don't get a cell phone number in your home area code. There's no need to provide geographic information about yourself via your phone number. I recommend choosing a dense urban area code with which you have little to no ties and go with that. A second choice is to go with the area code of a city where you used to live but are no longer resident. This would be consistent with your "pattern of life" without revealing current location data.

Pattern of Life

Eventually your number will start to bind to your identity. There's almost no way around it unless you have some very extreme disassociation of your phone from your known locations. For most people its effectively impossible to achieve. That being said, you don't have to overshare. The following rules will help keep your phone number somewhat clean:

Don't use your new number for any account sign ups, profiles, or services

Don't post your number on the internet (c'mon guys)

Only give your number to people you know

Use your old number that you ported to VoIP for anything that is associated easily with your name

Don't call 800 (or 900) numbers with your cell phone number – most log the call and associate the number to your account by default

Never give your cell phone number to the Government. Any Government.

Payment

If you can, pay your cell phone bill with (privacy) crypto, Privacy.com, cash, or a corporate bank account not tied to your name. One of the quickest ways to reveal the identity of a number's owner is by looking at the payer details. All the carriers can see this information.

Was it bad? The above process can be done in a day once you have your plan. The bigger time consumer is updating your contacts that you switched numbers. It is a good opportunity to prune your personal network if you don't subscribe to the popularity theory of contact lists. I have 1114 contacts saved in my phone of which I get a text from about 3 on Christmas and half that on my birthday. It's safe to say that contacts with labels like "Mike – Chicago Conference (follow up)" from 2007 are okay not to update about your new ultra-private life. In fact, it's time to delete Mike.

Other than updating my contacts with my new number, the only real friction point is discovering that some of my "SMS-only" logins where I used my old number to receive 2FA codes caught on that I had moved the line to VoIP and forced me to provide a true cell phone number on the account. It's total data mining and I'd like to do an ambush video of me yelling at the CEO of one of these companies as he or she is arriving at Davos. I also don't like being on video and have some sense

of puritan decorum from all my years living in New England, so I don't see this happening.

Next Level Stuff

Did I stop with the "good enough" solution outlined above. No. I had to go three steps further. If you are looking to level up to a vein amount of cellular privacy I recommend the following:

1. Get a second carrier hidden number added to your phone and don't share it with anyone other than very close contacts. This way if you need to burn your new cell phone number that you gave to most of your contacts it won't impact your inner circle. Think of it as having a "Public" and a "Private" number. Below is how I have my phone set up with two lines. I redacted everything that would be of use but I'm still giving myself credit for breaking up the wordiness of this article with a picture.
2. Get a cellular data Access Point Name (APN) to route your cellular data encrypted through a private network. There are several companies that provide this service. The advantage of an APN is that it encrypts and routes your cellular data by default and its always on. Think of it like a VPN for your SIM card. Halo's APN also splits your traffic into-session based post quantum encrypted tunnels and disperses the routes randomly, terminating at various egress points around the world. It's some Jason Bourne stuff, if Jason Bourne lived in 2030.
3. Carry a second cell phone to quarantine the "bad" apps that you need but don't trust. Carrying a second cell phone is wildly annoying. I do it because there are a couple apps I need for certain relationships or functions, but I

would never let them live on the same operating system as my main phone. For me, two examples of this are Signal & Telegram. I treat both of those apps as hostile, but I do have some friends and associates that contact me on either. The second phone allows me to have those apps while keeping them at arm's length. I don't put that phone on WiFi at my home or office and I don't ever give that phone "Local Network Access".

I need to be very explicit about one thing here. I don't care if you have a hundred extra phones, and you keep them all double faraday bagged in lockdown mode in an anechoic chamber under the ocean. There is no device on which you should ever have TikTok.

Conclusion: I think it's well worth the accrued privacy to pursue some variation of the cellular reset described above. It requires some tinkering and will be modestly disruptive. It will also cost somewhere between \$400-\$1600/ per year depending on what version of the above you select and assuming you DIY.

Returning to my initial point, your cell phone number is the primary attack vector against you in the digital world. So, before you bother with other privacy mechanisms like data base opt out, VPNs, living like a boss on Monero only, lay the foundation with a solid phone number set up. It's not as hard as it (may) sound. Also, Mike from the conference in Chicago, if you are reading this, I'm sorry I never followed up. ■

CAT AND MOUSE PART I: THE ATTACK FRAMEWORK

By Privacy Mike

It's easy for the average person to visualize a robbery or a home invasion. Self-defense instructors base their teachings upon the common understanding of what a physical attack looks like. However, most people don't know what "hacking" or digital stalking looks like. In order to defend against something, one must understand the attack. For educational purposes, I developed a framework to teach my students the fundamentals of how digital and privacy attackers operate.

This framework consists of three elements that form a Venn diagram. Each part intersects with one another. "You" are the middle of the framework because everything about you can be identified by combining the three points. These elements are location, thoughts, and associates.

Location

The most important element of the framework is your location. Knowing your location allows the digital attack to turn physical. If they know where you are at a given time, they can go to you and hit you with a \$5 wrench until you hand over your bitcoin wallet password or confess to a crime you didn't commit. In the case of a state actor, they can imprison you. In the case of violent criminal actors, they can assault or murder you.

Privacy enthusiasts go through great efforts to hide their location through the use of strategies such as using burner cell phones and buying things in cash with an alias name. Care is taken to avoid linking your home address with your name. Most effort from privacy enthusiasts focuses on concealing their location because it is perceived as the most important of the three tiers.

Thoughts

The "thoughts" element relates to whatever is on your mind. Perhaps you've hidden your location and the attackers cannot find you. But if they can find out what you're thinking, they can extrapolate where you are or where you will be in the future.

You may have your location fully hidden but if I know you have a toothache, I know you'll be going to your dentist and can wait there for you. If I know you're craving pizza, I can wait for you at your favorite pizzeria.

How does an attacker find out what you're thinking? There are many possibilities. You posted it to social media. You did a google search while logged into to an account in your name. You surfed the internet without a VPN and your ISP or cell phone provider knows what websites you visited.

Your historical financial transactions show patterns. Maybe you don't have a cell phone linked to your name but if I see every Thursday night you spend \$15 at the same coffee shop on a credit card, then I know where to find you next Thursday. And if I learn that the coffee shop hosts an event every Thursday night catering to a club of some kind, then I know more about what you're thinking.

Knowing your thoughts isn't just a way to find your location. It's also a way to manipulate your behavior. A spear phishing attack of a strategically crafted email related to your specific interests or concerns may get you to click a malicious link. A sophisticated attacker may plant an actor in a public place you're known to be with a false backstory that would pique your particular interests and get you to invite them into your life. Knowing your thoughts is a prerequisite for controlling you.

Associates

Associates are anyone and everyone you interact with — Friends, family, coworkers, neighbors, intramural sports team mates, video game guild members, etc. If an attacker can't track you, they may be able to track your associates. And eventually, your associates will lead them to you.

The concept of "associates" can be expanded out to regulars at your gym, cashiers at your grocery store, baristas at your coffee shop, and other people that see you in public on a regular basis in your community that you don't have personal relationships with.

The attacker may be a state actor with government credentials that shows your photo to everyone in your local grocery store, coffee shop, and gym. Maybe you've temporarily gone into hiding and one of these expanded associates noticed you sneaking around near your current safe house.

The attacker may be a civilian with false credentials posing as a state actor. Alternatively, they may leverage a social engineering attack to gain sympathy from community members. Don't think of associates as simply the people you know. Even in big cities, there are strangers who recognize you on a daily basis.

Framework Interpretations

This article initially presented the framework to the reader from the perspective of an attacker specifically targeting you and desiring your location. The attacker may leverage your thoughts and associates to find your location.

However, it may be that the attacker does not know who you are at the start of their operation. There may not even be an individual target in mind. The

attacker may be after a people who are part of a certain ideology, or in the case of genocide, part of a certain religion or race.

In this case, the attacker is not targeting you as an individual. They are starting with the “thoughts” point of the framework. Potentially also working over to “associates” to round up more people that are part of your group.

The attackers may have identified your ideology because of an internet search or because you sent a specific phrase over plain text SMS messaging. You may be a member of an online forum or Facebook group. They have your thoughts and now they want you.

It’s also possible that the attacker’s use of the framework starts under the “associations” tier and works backward from there. For example, imagine a political protest. You attend but have good operational security. You don’t bring a phone so there’s no digital trail. You wear a baseball hat and sunglasses to deter facial recognition. You travel to and from the protest discreetly. But a dozen of your friends are also there with you. And they don’t take this stuff as seriously as you.

The attackers have video of the protest and are unable to identify you. But your friends are privacy muggles. The attacker easily tracks down your friends, and then leverages your associates to identify you from the surveillance footage, in spite of your efforts.

The attackers do not need to coerce your friends to give up your identity. They can simply look at your friends’ cloud-stored phone contact lists and notice that you happen to be on all ten of their contact lists, and you are of the same age, gender, and registered voting party as them.

Suppose you didn’t even attend this protest. You stayed home. But all your friends went. The government arrests your friends and then identifies their associates, which includes you, and then arrests you as a potential future dissident. After all, you probably have the same “dangerous” political views as your friends.

The elements of thoughts, location and associates overlap to allow inferences to be made. If I know your location is at a gun range every Wednesday afternoon at 1pm during

your lunch break, I can infer your political leanings (thoughts).

With location I can also infer your associates. Maybe I dump cell tower records and I see there are two other people who go to the same gun range every Wednesday at 1pm. I also notice that all three of your cell phones are pinging the tower from the same dive bar on the other side of town once a month. Based on your location alone, I can find your thoughts and your associates.

Conclusions

Most people, even privacy enthusiasts, don’t understand how attackers operate. Understanding the offense helps you prepare a defense. The three elements of the attack framework intersect to paint a full picture of you. Focusing efforts only on concealing your location will not deter a sophisticated and motivated attacker who can leverage your thoughts and associates against you.

The next part of this series will discuss a defense framework. See you next time, friends. ■

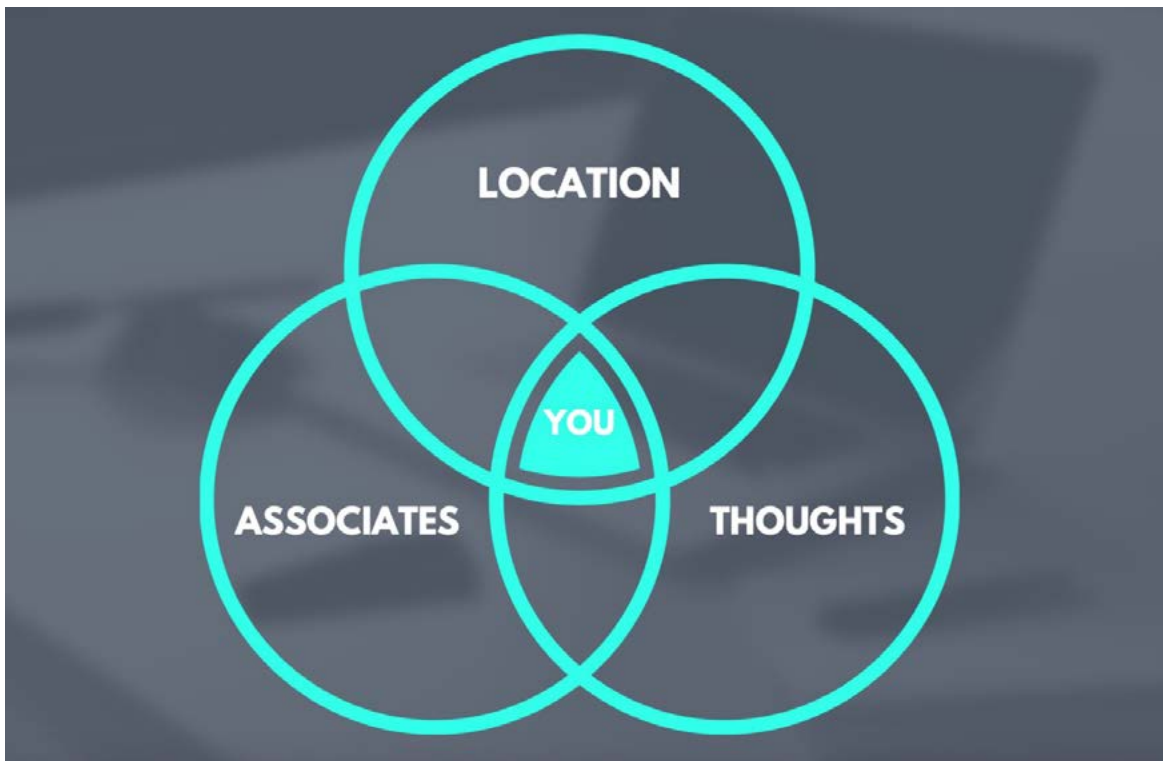




Image: Dan Dimmock

THE OSINT CORNER └

OSINT BEST PRACTICES FROM THE CLIENT'S PERSPECTIVE

By Jason Edison

Jason instructs live and online open-source intelligence courses for IntelTechniques in addition to working as a cyber-crime detective for a large U.S. police department. Each issue will feature an OSINT tactic from the IntelTechniques online training.

One of the unexpected benefits of running our OSIP certification program has been the opportunity to sit on the other side of the table in the role of the client rather than investigator. Participating in the completion of a real-world OSINT assignment from this new perspective has been eye-opening. The unique opportunity to observe so many different professionals working against real-world OSINT assignments has resulted in distinct patterns emerging among those who are successful and those who struggle. I want to share some of the key takeaways which have changed of my own approaches to client interactions and discuss how the focus of our training curriculum will shift to include a more modules which support the entire engagement process, from intake to delivering a solid intelligence product.

At this point in managing the certification program, I can well predict how most participants will fare before they submit their final reports. Ours is not an academic, multiple choice type

test that you see in most certification programs; we require our candidates to work a full OSINT engagement from intake to polished report. What I have found over time is that how people handle being onboarded to the program is a strong indicator of the level of professionalism and care we will see in their final report. So, in the spirit of helping us all improve, I would like to share my observations as well as feedback from participants themselves. Even if you do not plan to tackle our certification, you may relate to or benefit from some of the best practices highlighted in this article. Note: I will refer to "clients" in these examples and you should keep in mind that this can refer to anyone for whom you are doing professional OSINT work, including a colleague or boss.

Context

For those unfamiliar with our certification program, let us break down how the program works for context. The goal of the program is to replicate real

OSINT professional scenarios so that we can accurately gauge proficiencies and capabilities.

- It consists of a real world practical OSINT assignment which must be completed within a pre-scheduled ten day window.
- The participants must correspond with a "client" and clarify expectations, mission priorities, and any restrictions, such as deadlines.
- A full report is evaluated based on a standard of "worth paying for." Would a client be happy to pay for this report? Was the intelligence comprehensive and actionable? Was it error-free and professional?
- A key difference between this program and others is that it is not simply an academic exam, and therefore, passing requires not only technical skills, but also "soft skills" such as organization and communication.

- I run every assessment personally, so I have the benefit of seeing a wide range of approaches to and execution of these OSINT engagements.

Patterns of Success

In our line of work, we are used to paying attention to patterns, and managing our training programs is no different. We pay attention to not only direct feedback from our members, but also more subtle patterns that emerge with our most successful participants. It does not mean that every person that displays these patterns is guaranteed to pass, but there is a strong correlation between the level of diligence at the start of the engagement and the quality of product received at the end.

Attention to Detail – When we onboard someone to our certification program, we provide them with extensive instructions about the process and the program expectations. People who follow the onboarding instructions and respond accordingly from the start tend to pass the assessment. Organization and attention to detail are key characteristics that result in a great final work product.

Communication – Although we do not want to overly pester our clients, we should not be shy about requesting clarification on mission priorities and expectations. This not only results in a fine-tuned product, but it demonstrates professionalism and that you care about the client's needs. Written communications should be on point and concise, but there may be times where scheduling a call is more efficient than passing emails back and forth (especially if the work is sensitive and requires tighter operational security).

Written Verification – In almost every case, it is appropriate to establish expectations in writing. This becomes especially important if the client disputes your final work product, but it can also be handy during an engagement if you find yourself losing track of the primary mission goals. This can be anything from a binding contract to a simple email.

Practice Runs – I consider the first attempt at any new skill a prototype run based on “the pancake rule.” In any batch of cooking, the first one in the pan usually is the worst because we tend to adjust our technique based on the results of our early attempts. Intelligence work is no different. You do not want a paying gig to be the first time you have written a 40-page intelligence report. Practice is a key marker of success.

Learn & Adjust – We all have various strengths and limitations, but often, what makes the difference is when we can learn from our mistakes and modify our approach. Following a less-than-glowing performance, successful people will ask for feedback on how to improve versus asking for us to overlook the substandard results from their first attempt. People who are open to constructive (and sometimes critical) feedback and are willing to put in the work to correct themselves will most always knock the ball out of the park on their next engagement.

Patterns of Concern

Just as there are patterns that have emerged when looking at our most successful participants, there are also signs that often indicate potential problems accomplishing our mission.

Narrow Skillset – We tend to drastically undervalue those “soft skills” such as communication and documentation. The focus in OSINT tends to be all search, but if you want to get paid, it is not enough to just be able to find the intelligence. You need to be able to identify and articulate the actionable intelligence. Remember, information is only intelligence once it has context, and we are responsible for illustrating that context.

Excuses – Whenever anyone provides excuses prior to starting the engagement, this is a bad sign. It almost never ends well, and you would be better off turning down the assignment up front if you are already telling your client why it may not result in a solid intelligence product. If a client is paying me for work, then

it is not their problem that I might have some obstacles to negotiate to accomplish the mission. (This is not to be confused with clarifying limitations due to things like policies or law, which is appropriate.)

Expecting a Second Chance – We always look at an engagement as an opportunity to win or lose a client's future business. Do not plan on or assume you will be given a second chance to correct and improve your work. Deliver quality work on time and assume anything less will lose you that client.

Lack of Preparation – If you wait until the middle of a critical investigation to use a special tool or service for the first time, it is almost guaranteed to not work as expected. Every tool in our belt should be tested well ahead of time, and we should arm ourselves with a good framework for research and documentation. You do not want to spend valuable investigative time reformatting and customizing report templates or troubleshooting why archive.org is not returning expected results.

Time Management – This can be incredibly challenging, especially while you are still building experience. The truth is that we often cannot guess how long an OSINT engagement might take, but that does not alleviate our responsibility to meet any deadlines. If you are ever approaching a deadline that you cannot meet at a level of quality that you are comfortable with, you must communicate with your client immediately. There may be a chance for an extension, but we do not wait until we miss a deadline to open the conversation.

Quality Control – I am no longer surprised by the number of reports that I receive that are riddled with spelling and grammatical errors. This is unacceptable in a professional intelligence report. We should always use a combination of technological and human resources to check our work. I typically use MS Word's Editor function for my first proofing pass and then ask at least one trusted colleague to also

review the report for both form and content.

Lack of Proper Sourcing – This line item is pretty specific to OSINT and research, but just keep in mind how much context matters in our intelligence work. In most scenarios, failure to source your work will result in a weaker intelligence product. I cannot think of many missions for which the source of the intelligence did not matter.

Participant Feedback

We have collected feedback from participants over the last two years, and the following are some consistent patterns in what our investigators had to say.

- The average time split between research and documentation phases was roughly 70/30. That means that most people submitting quality work set aside almost a third of their available time for writing and quality control on their reports.
- For a large assignment, such as ones which required the investigators to compile OSINT profiles on multiple targets within a group or organization, most people spent more than thirty hours on the mission, from intake to finished work product.
- Many participants mentioned that either they prepared tools and templates ahead of time or they wished they had. Having burner accounts, reliable search sites, and documentation templates ready to go is a huge time saver when you are working under a deadline.
- As mentioned above, many successful participants who lacked real world experience put themselves through some practice runs, which helped them iron out any bugs in their research and/or documentation procedures.
- Know when to take a break and get some rest. There are points of diminishing returns

when hammering away on an engagement. Know when to take a break or call it a night. A rested brain can dramatically reduce errors and other inefficiencies. One participant articulated this well by stating “validate your OSINT methodology” before tackling a time-sensitive assignment.

- Different targets may require variances in how you approach your research. There are many cultural and lifestyle factors which affect the effectiveness of certain investigative tactics.

Hopefully, some of these observations will help you fine-tune your own OSINT contracts and operations. If nothing else, occasionally review your own client interactions, and ask yourself if you are being responsive with communications, addressing the priorities laid out in the contract or scope of work, and being diligent when it comes to quality control on the final work product. ■

OSINT & Privacy Video Training

100+ Hours of Video Training | Optional OSIP Certification

Register at IntelTechniques.net

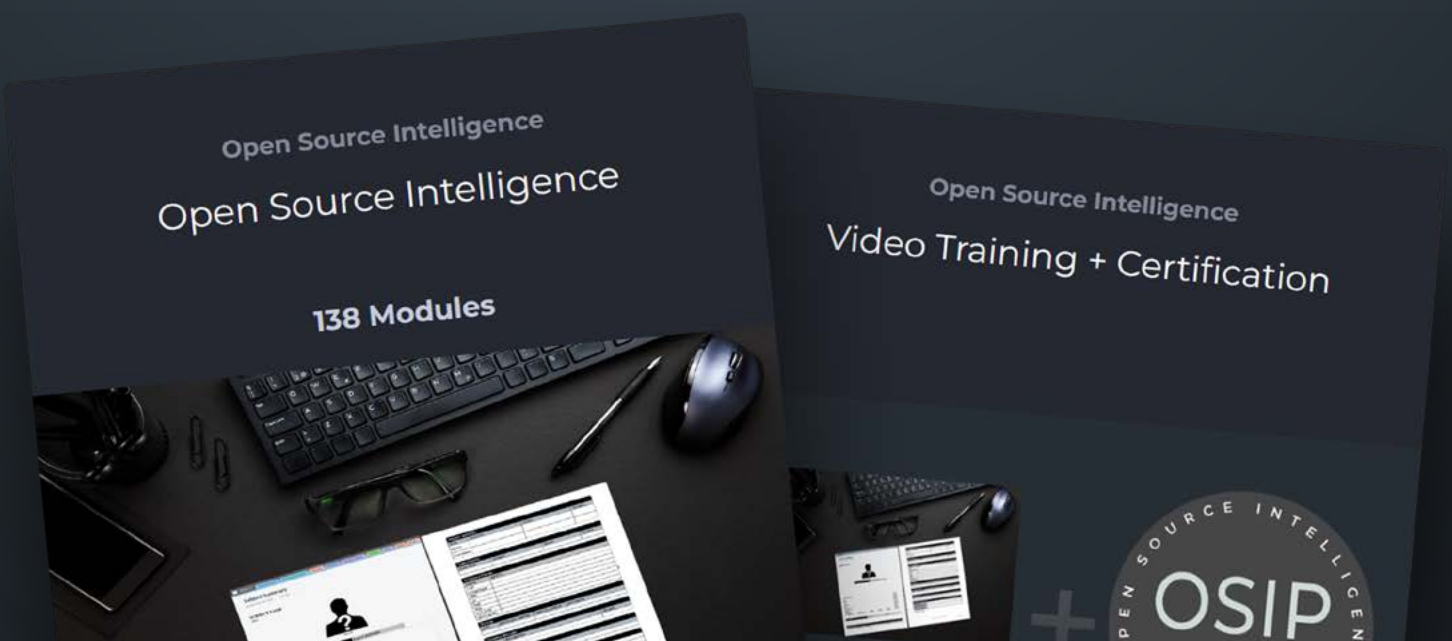




Image: Vidar Nordli-Mathisen

HUNTING APPS FOR OSINT

By HeckSec

Technology advancements have impacted every aspect of the world since the dotcom boom of the early 2000's. Virtually all industries have capitalized on this boom and the outdoors industry is no exception. Technology has changed the way hunter's hunt; GPS improvements (smaller, more accurate), clothing (lighter, stronger, with scent technology), and weaponry (lighter, stronger, cheaper, etc), to name a few.

In the last ten years there has been a surge of web and mobile applications that were designed to aid outdoor advocates in planning, scouting, and

executing successful hunts. Hunting and land management apps such as OnXHunt (<https://www.onxmaps.com/hunt/app>) and HuntStand (<https://www.huntstand.com/>) offer users the ability to search for properties by ownership and location. These apps provide helpful information to hunters, but this short article will show you how their standard features can be leveraged to identify property ownership information during OSINT investigations. For example, it is possible for a private investigator to locate property owners for a client, or a journalist to tie an LLC to a specific property. Although there are other applications that can provide property

information (such as Zillow or Redfin), these apps are limited in that they do not provide ownership information.

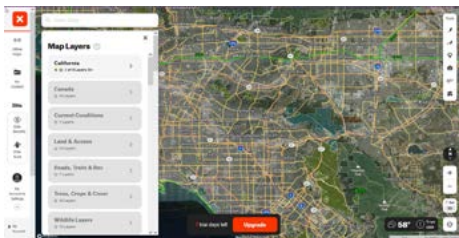
All of the examples and screenshots provided were created using the OnX Hunt web application. The app is available on Android devices, iOS devices, and as a web application. All information in this article was gathered by using a free trial. The trial is offered to new users after creating a free account. The account was created by providing an ephemeral email address from a free online email service. No credit card information required! HuntStand has also been confirmed to offer property ownership information. Although

HuntStand has similar features and functionality, it is not featured in this article. There was effort to redact the full names of all property owners in the images used for this article.

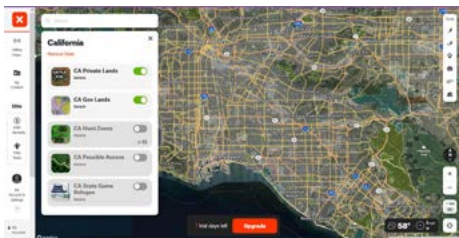
App Features

There are many different features within the OnX Hunt app, but this article highlights map layers, location searches, and owner searches.

This Image (Image 01) provides insight into available map layers. A user can choose specific states (or Canada) to focus on and select conditions such as air quality, smoke forecast, slope angles, and trails.

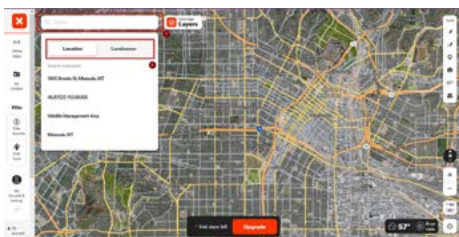


This image (Image 02) highlights options within the California map layer. Notice the "CA Private Lands" layer option. This is the specific layer that makes hunting apps valuable for OSINT investigations. Make sure this layer is turned on before continuing.

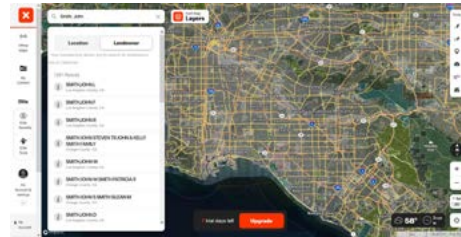


People & Places

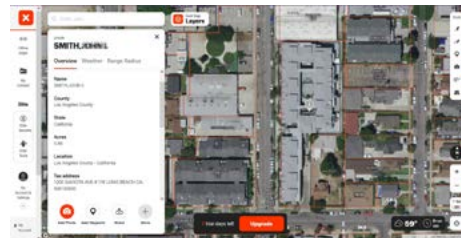
Clicking on the search box near the top left allows users to search by property location or property owner. (Image 03)



While searching for landowners, the app will suggest results (The name John Smith was only used as an example). (Image 04)



Clicking on a landowner's name will take the user to the property in question. The app will provide Name, County, State, Acres, Location, and a Tax Address. In Image 05, the names of property owners have been redacted. Notice some of the properties are owned by LLCs. An LLC can be a great privacy tool for assets if used correctly. Michael Bazzell discusses this topic at length in his book, Extreme Privacy: What It Takes to Disappear.



The power of these apps is also showcased by the ability to add waypoints (tag specific locations) and draw boundaries. Hunters use these features to build and plan hunting trips, while an OSINT practitioner can use them to organize investigations.

Although the OSINT benefits of hunting apps are clear, no tool is perfect. At times, information may be outdated. One could argue that all information during an investigation should be cross-referenced with other tools and techniques to prove validity. With regards to property information within these hunting apps, old public records could be to blame for outdated property. Apps could also reflect outdated information if they are slow to update their backend services. The following section discusses this

potential obstacle using Dodger Stadium as an example.

Using the app's location search feature, a user can easily find Dodger Stadium (the app will zoom into the location of the property once it's selected from the search suggestions). In image 06, the app displays the stadium owner as Realco Intermediary LLC, which isn't correct. A quick google search indicates that Frank McCourt, the previous owner of the LA Dodgers, was an officer of this LLC at some point. The issue is that Frank sold the Dodgers to Guggenheim Baseball Management in 2012. Although the Dodgers have had new ownership since 2012, this snippet from Wikipedia may explain the lack of property ownership changes within the OnX app (and thus public record); "According to Guggenheim Baseball Management, McCourt will have no control or influence over the land, but will profit from potential future development of it."



This is only a theory and does not prove that all property information is inaccurate. Feel free to validate the information provided by the app by searching for yourself, your family members, or friends and neighbors.

The original intent of these apps and their features was not to feed the paranoia of the privacy-conscious technologist. Hunters all over North America have used these apps to ask landowners permission to hunt on private land. Outdoors men & women have clearly benefited from the breadth of technology improvements imposed on hunting gear and apps in the last decade. In this case the improvements can be a valuable addition to an OSINT professional's toolbox. ■

ELASTICHUNT: THE TOOL THAT MAKES DATABASE HUNTING EASIER

By EF1500

As an OSINT researcher, you know the importance of combing through these treasure troves of data to uncover key insights on everything from individuals to major corporations. But let's face it - the process of accessing this information can be excruciatingly difficult and time-consuming, and the prospect of discovering truly undiscovered information can seem nearly impossible.

But what if there was a better way? If you're intrigued by the idea of streamlining your database searching process and uncovering new and valuable insights, then this article is for you.

While reading Michael Bazzell's "Open Source Intelligence Techniques," I stumbled upon a section on elastic databases. I was amazed by the sheer amount of data that was available, just waiting to be explored. The tool (<https://github.com/AmlJesse/Elasticsearch-Crawler>) Bazzell presented to download these databases worked flawlessly, but the real kicker was just how difficult it was to actually find these databases and extract any valuable information from them.

Undeterred, I set out on a mission to find as many databases as I could. I wrote a script to check if an IP address had an elastic database and I spent hours on end scanning the internet with masscan, hoping to stumble upon some hidden treasure. But for the longest time, I was getting nothing. Every scan was coming up empty, and I was starting to feel hopeless.

That all changed the next day when my script finally found something. And then another, and another, until they were popping up left and right. I was finding all kinds of databases, some of them containing highly sensitive information. It was a thrilling experience, and I knew I had stumbled upon something truly valuable.

But unfortunately, the process was incredibly time-consuming. I was going back and forth between scripts and programs, copying, pasting, trying to find something interesting. It was exhausting, and I knew there had to be a better way. That's when I decided to create Elastichunt, a tool that could search, locate, and download databases all in one place.

My aim with Elastichunt is to create a versatile "swiss army knife" of Elasticsearch databases that enables the user to search, locate, and download these databases all in one place. That way, no longer will you have to tirelessly go back and forth between scripts and programs, trying to find something interesting.

To get started, you'll need to clone the repository from the following link:

<https://github.com/ef1500/Elastichunt>

Once you've cloned the repository, you'll need to install the necessary requirements by running the following command in your terminal:

```
python3 -m pip install -r requirements.txt.
```

To search for databases, you'll need to run a command in your terminal. The command looks like this:

```
python3 elastichunt.py  
192.168.0.0/16 9200 --elast-  
ictimeout 16 --scannertimeout  
16.
```

The first part of the command specifies the IP address or IP range you want to search. The second part specifies the port number to search for databases on. The last two parts specify the timeout for the elastic API and the scanner, respectively. You can adjust these values as needed, but it's generally best to keep them above 10.

If you want to scan a large part of the internet, it's important to be careful so that you don't crash your computer or get disappointing results. To help with this, Elastichunt provides the option to split the scan into smaller "subscans" using the --staged option. This splits the IP range into smaller CIDR ranges to make the scan more manageable. For example, 192.0.0.0/8 would be split into 256 stages of the /16 subnet, 192.0.0.0/16, 192.1.0.0/16 ... 192.255.0.0/16.

I think that the most powerful option though is using filters. You can define your own filters, and you can quickly get the indices that are most important to you. To make a filter, you just need to make a filters.json file (there should already be one from when you cloned the repo) and you can define filters like so:

```
[
  {
    "filter_name": "allowed_indices",
    "filter_type": "regex",
    "field_name": "index",
    "filter_items": ["customer", "user",
"spreadlog", "leads", "resume", "employee",
"hospital", "passport", "voter", "resident",
"billing", "debt"]
  },
  {
    "filter_name": "allowed_filesizes",
    "filter_type": "regex",
    "field_name": "store_size",
    "filter_items": ["mb", "gb"]
  }
]
```

The filter_name can be anything you want, it's just there to help you remember what the filter is for. The filter_type tells the program what type of filter to use (currently the

only supported one is regex). Field_name is the field you want to filter on. This has nothing to do with the field names contained inside the index, it only has to do with the index itself. Possible field names are: health, status, index, uuid, pri, rep, docs_count, docs_deleted, store_size and pri_store_size. The filter_items are the things you're interested in. The program will look for indices that have those items in the field_name you specify.

Once you've created your filters.json file, you can include it in your searches by adding the --filters=filters.json option to the Elastichunt command. For example, your search command might look like this: python3 elastichunt.py 192.168.0.0/16 9200 --elasticsearch 16 --scannertimeout 16 --filters=filters.json.

Using Elastichunt, I've been able to ingest a staggering amount of indexes, many of which contained highly sensitive information. It's saved me an immense amount of time and made my work as an OSINT researcher much more efficient.

As I continue to work on Elastichunt, I plan to make major updates and additions to the tool in the coming months and weeks. And I welcome any feedback from the community as we work together to make this tool the best it can be.

Thank you for taking the time to read this article, and I hope you found it informative and inspiring. Let's continue to push the boundaries of open-source intelligence together! ■

OSINT & Privacy Digital Books



Original Books

Digital Supplements with Free Lifetime Updates

- ✓ 7 Digital PDF eBooks
- ✓ Free Updates to Digital Supplements
- ✓ Over 1,600 Pages at 8.5" x 11"
- ✓ Our Full Playbooks
- ✓ Available as Gifts
- ✓ Updated Content

Order at IntelTechniques.com



Image: Glenn Carstens-Peters

CUTTING DOWN ON BROWSER EXTENSIONS

by Alex Barista

Browser extensions, usually maintained by third parties, add value for users who are missing features in their web browser. Extensions also increase the attack surface of a browser, require trust in the developer, and make you stand out more.

I had a bunch of add-ons installed some time ago with very specific little jobs. Maybe they changed the look of a web page, helped with frequent downloads, or allowed automatic translation. Today, I can gladly do without such helpers in exchange for not weakening my privacy and security. For the remaining services I had an extension for: a password manager, a spell-checker and a read it later service, I now use the desktop application, the web version and a bookmarklet.

After renouncing **normal** extensions, I started to collect privacy extensions instead. I searched for the most popular Firefox add-ons in this category to see what data I could block or seemingly randomize. Today I have learned that a single extension and the right browser settings can take care of most of these functions, and I don't consider the remaining ones as useful to me anymore.

Getting rid of duplicates

uBlock Origin (uBO), a content blocker created and maintained by Raymond Hill (gorhill), will replace quite a few add-on categories by itself. This blocker convinces me and many others technically as well as regarding licensing (GPLv3), mindset and its history. The uBlock Origin default setting is called Easy mode and relies on static filter lists, replacing all other ad blocker

extensions. With the Medium mode activated, 3rd-party scripts and 3rd-party frames are additionally blocked dynamically, replacing all other script blocker extensions. In Hard mode, 3rd-party in general is blocked, replacing all other cross-site request blocker extensions. You'll find how to enable the different modes and which one is right for you at <https://github.com/gorhill/uBlock/wiki/Blocking-mode>.

To get pages to work with uBlock Origin I use the integrated logger with the filters ****blocked****, ****image****, ****script**** and ****3rd party****. Holding shift, you can open the logger in a tab if you don't have much screen real estate.

Note on filter lists

Filter lists can be read (proof of concept at <https://browserleaks.com/proxy>) and thus simplify tracking for an adversary. This can be especially revealing if

you enable filter lists specific to your language or country. There have also been security concerns regarding malicious 3rd-party lists. I recommend using only the preselected and needed filter lists for each mode, or additionally, just the preinstalled ones. Interestingly, in Hard mode, browserleaks.com shows all installed lists, but as soon as 3rd-party is allowed (equivalent to Medium mode) the page shows only the ones that are activated.

Replacing other privacy extensions

If you are using a JavaScript toggle extension, you can replace it with the uBO setting **Disable JavaScript** and toggle it per site in the popup user interface.

If you want to get rid of the cookie pop-ups, you can activate the integrated **uBlock filters – Cookie Notices** list and / or the **AdGuard – Cookie Notices** list. No additional extension is needed.

Add-ons that strip tracking parameters from URLs can be replaced by uBlock Origin's integrated list **AdGuard URL Tracking Protection**.

Extensions that change HTTP requests to encrypted HTTPS ones are no longer necessary with the Firefox setting **Privacy & Security - Security - HTTPS-Only Mode - Enable HTTPS-Only Mode in all windows**.

Anti-fingerprinting tools can be replaced with Resist Fingerprinting by enabling the Firefox setting **Privacy & Security - Browser Privacy - Enhanced Tracking Protection - Strict**. This might break some web pages, you can disable the enhanced protection on a per-site level.

Making the remaining extensions redundant

You can let tracking companies gather some of your information, as long as they can't put it together. A good way to achieve this is by isolating your browser tabs from one another. This does protect against so many tracking approaches that it can be used to reasonably replace container, local

CDN, redirect, and cookie manager extensions. Enable Total Cookie Protection and Enhanced Cookie Clearing (again by enabling **Privacy & Security - Browser Privacy - Enhanced Tracking Protection - Strict**) and Site Isolation (should now be enabled by default, put **about:config** into the address bar and check that **fission.autostart = true**).

Implementing private browser settings

We now have all the main privacy extension categories replaced by uBO and Firefox settings. This approach did not perfectly duplicate every feature. Being able to cut down on browser extensions should make up for that.

To implement these strategies, you could harden a Firefox profile by yourself. I suggest a ready-to-go script that loads privacy-friendly settings at the start of Firefox instead. The arkenfox user.js is a popular one, with comprehensive documentation and frequent updates (<https://github.com/arkenfox/user.js>). Extract the archive in your newly created Firefox profile and optionally override settings that are too strict or not strict enough for your use case. Then install uBlock Origin and activate your preferred mode. For additional compartmentalization, add multiple Firefox profiles for different uses like browsing, logins, research, and work. Type **about:profiles** into the address bar to manage and switch between your profiles.

Adding the Tor Browser to the mix

If you use the Tor Browser, you should not alter it because that would make you stand out from other users. That means you can't use uBlock Origin since it's not preinstalled. Instead, there is NoScript installed, another capable content blocker. NoScript is mostly disabled by default. I'm completely fine with both of this. The extensive isolation and anonymization that the Tor Browser provides make any content blocker or other privacy extension unnecessary. If you need to protect against scripts, you can change the NoScript preferences indirectly in the

Tor Browser Settings. Choose **Privacy & Security - Security - Security Level - Safest** to block JavaScript by default. Be aware that you can be fingerprinted by what you block and allow. That is why the overrides you make in the Tor Browser version of NoScript are only temporary.

The Mullvad Browser as an alternative

A partnership between Mullvad VPN and the Tor Browser, the Mullvad Browser is practically a Tor Browser without Tor and with uBlock Origin preinstalled. It can act as a ready-to-go solution for a secure and user-friendly browser for many use cases. As the Tor Browser, MB should be left as is. This all means less flexibility than a custom Firefox build but also better privacy enhancements through the Tor Project.

Putting it all together

For the most protection, ideally use the Tor Browser. However, there are valid concerns for some not to use Tor (at least without bridges) because simply being identified as a Tor user by their ISP could get them into trouble. There are also some web pages that will not work over Tor, and the Tor network is not meant for bandwidth-intensive browsing like streaming video or audio. All of this means that the Tor Browser is not a replacement but rather an additional tool. For daily browsing that is not suited for the Tor Browser, I recommend Mullvad Browser. For everything that breaks or for logins, I suggest building different profiles per use case on a vanilla Firefox with uBlock Origin and arkenfox.

With uBlock Origin, arkenfox, Firefox profiles, Mullvad Browser and the Tor Browser you should be able to implement a private browsing strategy that suits your needs. This guide is centered around the desktop version of Mozilla Firefox. The very different mobile browsers and the limited environment they work in need their own strategies. More on that, maybe another time. ■

**YOU DON'T NEED A
WEBSITE. YOU NEED
RESULTS.**

**Privacy-focused websites
that drive outcomes.**



Astropost

Astropost is the official design partner for this issue of UNREDACTED MAGAZINE. Need an ad designed for the magazine? Or a website that gives you results? We'll help you out!

OSINT EXPLORING WITH MEALTRAIN

By Anonymous

I am currently enrolled in the IntelTechniques OSINT training and the biggest lesson I have learned is that there are OSINT opportunities behind almost everything. The other day I got an email from my church. They were planning a potluck and they gave everybody a link to a site called MealTrain. MealTrain's site says:

MealTrain.com allows members to organize a meal calendar for a friend after a birth, surgery, illness, etc. This calendar helps organize friends and family members who want to sign up for a date and make and deliver a meal. The organizer can add a story and a photo as well as make regular updates. Once the page is created, MealTrain.com allows users to share their page with friends and family through integrated social network links (Facebook, Instagram, etc.), e-mail, posters, sms, and an internal messaging tool. Invited participants can then view the calendar, review the recipients food preferences and sign up for a date to provide a meal.

They also started allowing potlucks to be posted. The link I received was in the format of (not an active link):

<https://www.mealtrain.com/potlucks/k4mz/flyer>

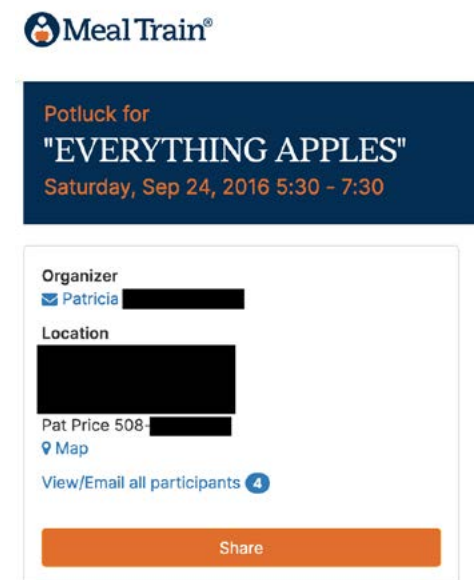
Clicking the link took me to a flyer for the event which was already set to print from my browser. It looked like:



I never scan a barcode from my device so I just removed the word flyer like so:

<https://www.mealtrain.com/potlucks/k4mz/>

This immediately opened the event and allowed me to see the location for the event like so:



This location is a somewhat public building so I didn't really care about that. What I was most interested in was the following.

Appetizers

This slot is still available

-  Susan [redacted]
Cheese and Crackers
-  Deborah [redacted]
Pumpkin Squash Apple Soup
-  Patricia [redacted]
Deviled eggs

Salads

This slot is still available

-  Patricia [redacted]
Tossed salad
(Prepared by Carole [redacted])
-  [redacted]
Apple salad
(Prepared by Debbie [redacted])
-  [redacted]
Waldorf salad
(Prepared by [redacted] Hernandez)

I could see anyone who had volunteered to bring a dish and the dish they were bringing. I assumed that I could only see this because I had received a message with a special hidden URL. Nope. This is all public information. I went straight to Google and searched:

site:mealtrain.com

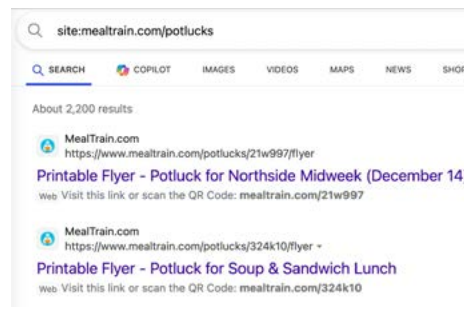
I got tons of hits, but they all required a login to the MealTrain website. Whew. But then I looked at some of the links Google was giving me. One was like:

<https://www.mealtrain.com/trains/nlryo/invite/>

If I just removed the word "invite", I saw the full post.



This tells me that detail pages are either at mealtrain.com/trains or mealtrain.com/potlucks. I then wondered how many of these pages have been indexed by Google. I searched `site:mealtrain.com/potlucks` and was disappointed (relieved) to see only eight entries. The training has taught me to never rely on Google. So, I tried Bing:



Holy. Cow. Over 2,000 active profiles announcing people's past and future locations and their favorite dishes to bring to a potluck. I played some more and discovered that any profile URL,

such as mealtrain.com/trains/06w4 could also be shortened to mealtrain.com/06w4. This presented even more search engine results.

While this seemed creepy and like a privacy invasion, what could anyone really do with this information? I think this is a hacker's, stalker's, or social engineer's dream. Imagine if I am trying to serve you a subpoena and find out where you will be next Saturday and what dish you are making. Maybe I will show up! Maybe I am a stalker and I will use this information at the next event to impress you with your favorite food. Maybe I am just a pest who will volunteer for every dish to be a nuisance.

Do we really NEED these types of services? What happened to a paper signup list or a phone call? ■

THE SECRET PRIVACY BENEFIT OF A COSTCO CARD

By Skeptical Sam II

When I originally joined Costco, I gladly handed over my driver's license when asked by the customer service clerk processing new memberships. A photo was taken and a new Costco membership card was issued on the spot that had a blurry image of my face on the back. Shortly after, I began receiving mailings from Costco to my home advertising monthly sales. Since then, I have moved many times and now live in another part of the country. I now use a PO Box for personal mail and packages are delivered to my home under an alternate name.

I have renewed my Costco membership annually, with the exception of a few gap periods, and I've never been asked to show my ID again. Since the original request for my ID was many years and many residences ago, I consider any privacy implications to be minimal for me. Costco has not had an accurate address, phone number or image of my current government ID in years and has no idea where I live. I always pay for my purchases in cash, including membership renewals. If I was to join today as a new member, I would use my passport card instead of a driver's license and a CMRA address (if you want the flyers). Obtaining a Costco membership under an alternate name may not be impossible, but would definitely require a fake ID or a

very lax membership clerk. I have not yet figured out how I could obtain a membership under an alternate name.

For those who choose to become a Costco member, there is a little-known privacy benefit of having a Costco card with your photo on it. I have been able to use my Costco card as a second form of "identification" at many establishments that demand an ID for service. When opening up a new mailbox at a local UPS Store a couple years ago, I was requested to present two forms of photo ID. I presented my passport card and then asked if my Costco card would serve as the second form of ID since "it has my photo on the back". The clerk looked at the card and said "oh yes, that will work fine." I verbally gave them the address of a nearby relative and my new mailbox and keys were issued. In this example, my Costco card served as a "2nd ID" and allowed me to withhold my driver's license.

This strategy has also worked at many medical facilities that demand an image of an ID for service. I have carried a passport card for years and that is my preferred method of ID when requested. However, I absolutely refuse to let anyone take an image of any valid government ID, including my passport or driver's license. In my opinion, there is no need for anyone to retain an image of a government credential,

which could be used for financial fraud or to unlock a credit freeze. Refusing a request to take an image of my ID usually becomes contentious and confrontational and I've even been told "I have to copy something". I've been successful in diffusing the situation by calmly explaining that "I was a victim of identity theft and my lawyer said I shouldn't let my ID be copied anymore." I then offer my Costco membership card and show that it had my name and photo on it. That has worked well many times for me, as the receptionist really doesn't care and just wants to complete the task.

It is unfortunate that the warehouse clubs demand a government ID for membership. After all, they aren't extending any credit to members and certainly a membership could be issued without any ID, as long as the annual fee is paid. As an extreme privacy enthusiast, nearly everything I purchase online is in an alternate name or the name of an entity, so I understand the resistance of many to establish an account in your real name. If you do decide to become a member, my suggestion is to use a passport for ID, a VOIP phone number and a CMRA mailing address. If you don't care to receive the sales flyers or to receive texts/calls from Costco, you can simply provide disinformation, such as the address and phone number of an apartment leasing office or YMCA. ■



POLYGLOT PASSWORDS

By Michael J. Ross

Anyone instructed to provide a new password for securing — and later accessing — some sort of account, faces the dilemma of coming up with a permutation of characters that match the conflicting criteria of being both memorable and yet long and cryptic enough to foil any hackers trying to guess or automatically generate potential matches. At least, this would be the case if not for the assistance of password managers, which are standalone programs or web browser features or add-ons that can generate and store a suggested strong password unique to each account. But even then, you need to dream up a strong master password to unlock the virtual vault formed by your chosen password manager, to access all of your other passwords.

There are countless strategies — and combinations thereof — for dreaming

up a worthy password. For instance, you could write down and memorize a seemingly random combination of letters and punctuation marks. But it would have to contain enough characters to be secure, and yet the greater the number of characters then the greater the likelihood that you would not be able to recall it in the future, especially under stress (e.g., moments before boarding an international flight when the gate agent insists that you provide the ticket number of your onward travel flight, as evidence that you do not plan to overstay your visa).

Alternatively, you could form a string of gibberish by concatenating the second letter of the first two dozen words of the lyrics from your favorite song. If you are compelled to type in that password at least once a day, to access your password manager, then you will likely never forget your technique for re-creating it each time. But if for some reason you only need to

remember that password infrequently, will you always remember the number of words you chose to use, before your unsuccessful attempts lock you out of your account? And how did you decide to handle single-character words? Come to think of it, did you decide after all to tack on your birth year or a punctuation character?

A more straightforward password could be had by simply using the words themselves, and not a pattern of characters and with no embellishments. The result would be much easier for you to remember, but sadly also much easier for attackers to correctly guess, because typically, after they first try all of the most commonly-used passwords (from numerous lists published online), they will then programmatically try combinations of words from a dictionary — hence the term “dictionary attack”.

The computational power now available for such attacks allows for

millions if not billions of guesses to be tried per second, depending upon the hardware, at least for off-line efforts in which the attackers can use password-cracking programs against a locally-stored file (such as a leaked database) containing the encrypted passwords of multiple accounts, including yours. Users can attempt to make passwords longer and stronger by employing more words from the dictionary, but attackers can improve their results by employing more robust hardware — in something of a digital arms race.

Naturally, attackers use the dictionary of whichever human language is associated with most if not all of the account owners. In those rare cases where most of the people targeted are bilingual, then one would expect the attackers to use all of the dictionary words of both languages — or at least the most commonly used words, to greatly diminish the number of possible permutations without significantly diminishing the odds of success for the bulk of the hashed passwords.

There is, however, a potential counter-strategy I have not seen presented anywhere: Rather than limiting the candidate words to a single human language, choose words from many foreign languages — the more, the better — possibly with accented characters replaced with their closest non-accented equivalents.

For instance, you could concatenate some foreign translations of the word "hello": "bonjour" (French), "hallo" (German), "namaste" (Hindi), "ciao" (Italian), "nihao" (Mandarin Chinese), "privet" (Russian), and "hola" (Spanish). This would result in "helloworldhallonamasteciaonihaoprivethola", for a total of 43 characters. One could also add from less common languages, for instance: "salam" (Azerbaijani), "saluton" (Esperanto), "konnichiwa" (Japanese), "salve" (Latin), and "habari" (Swahili) — resulting in an even more secure password. In addition to natural human languages, you could also use synthetic ones, such as Klingon and Dothraki. Of

course, for devising your own password, you should use a base word other than "hello".

Reputable sources (e.g., Ethnologue) claim that there are many thousands of languages in existence and more than 150 that are each spoken by more than a million people. Would a significant portion of all password attackers ever expand their search space to incorporate the dictionary words from multiple languages? It is unlikely, because each language added would exponentially increase the possible permutations that they would need to test. Moreover, if their existing methods using only English continue to be largely successful, then it is inconceivable that attackers would massively increase their investment of time and computer resources simply to crack a few remaining stubborn passwords, such as a polyglot one.

Perhaps this is one more advantage to thinking beyond English. ■

**Are you in need of
answers that seem
just out of reach?**



CALABASH
INVESTIGATIVE CONSULTANTS, LLC

www.calabashllc.com
678.909.1955

Georgia Licensed
PDC002961/PDE052357



LOOKING BEYOND THE NUMBERS

Gustov1

Have you ever searched for a subject but just not producing many search results? I may have some nuggets for you.

I have been in the open-source intel and privacy world for the past two decades or so and have searched and removed my name and information off most websites but will sometimes continue locating some fragments. I always try techniques and different ways of looking for data. My dad always said, sometimes you cannot see the forest through the trees.

At the beginning of every year, I conduct a search of my name, address, etc. to see what is floating around on the Internet and work through Michael's Personal Data Removal Workbook. I also have trusted friends to do the same to check and verify my results.

I also use many different popular online search engines/tools like Google, Searx, Carrot, Archive.org, etc. during my search.

When opting out of most "people search" sites they will remove your information from the "public end" of the website, but the "opted out" information remains in the back end (opted out) part of the database.

During my most recent search I noticed on some of the "people search" web pages **result** numbers were higher than the actual **listed** results.

I observed these difference or fragments on Veripages (<https://veripages.com/>). According to domain records this website has been around since 2018. I requested to have my information removed from the page around that same time. But I noticed

some nuggets of information have remained over the years.

Use the example below while searching **Veripages** (<https://veripages.com/>).

<https://veripages.com/name/FirstName/LastName/#state-StateName>

Example- <https://veripages.com/name/FirstName/LastName/#state-NewMeixco>

Entering different variances of my first and last name gave different results.

As an example, **Amy Stewart** in Alaska.

The following URL - <https://veripages.com/name/Amy/Stewart/#state-Alaska>

It will display - "Found **10** people in Alaska."

On the left pane of the results page, you will see a **Filter by State** and a **number**. The number initially displayed does not always correlate with that state listed results.

Under the FILTER BY STATE section – select All states.

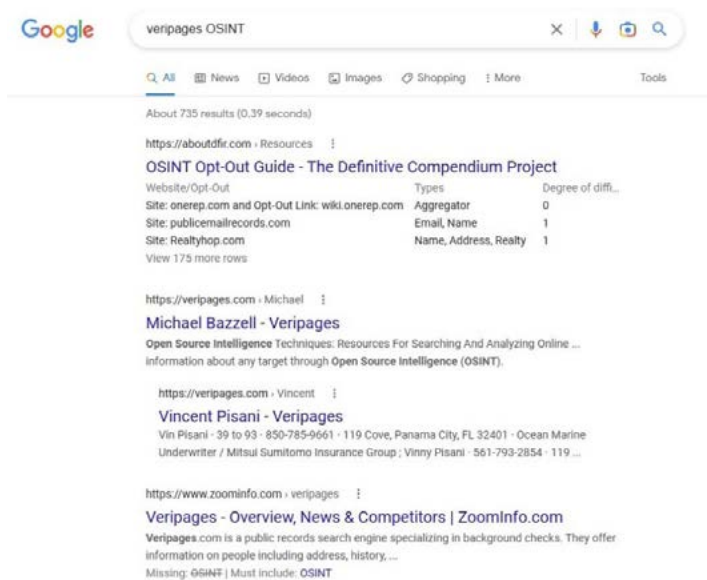
This will display all states under this section. DC shows eight results in the left pane but displays only “Found **7** People in DC.”. I have seen similar results with many of the searches I have done.

It appears Veripages is “removing” the requested “opt-out requests” but not resetting the total resulting numbers from their backend database.

In the case of my name – the state result displays ‘7’ but when clicking the state name – 13 cities are displaying. The three results were cities that I previously lived in. Selecting an individual city only displays positive or not redacted “hits” or results.

When searching for a subject that has information redacted from most people search websites you can use Veripages as a “pivot” point and possibly locate previous cities the subject may have lived.

Also, enter the “veripages OSINT” in Google and see the first couple interesting results.



I have also seen these similar results with the website **UnMask** <https://unmask.com/>.

<https://unmask.com/name/FirstName-LastName/stateinitials>

Example - <https://unmask.com/name/FirstName/LastName/AK>

Entering different variances of my first and last name gave different results.

Using Amy Stewart in Alaska as an example,

Enter - <https://unmask.com/Amy-Stewart/AK/> In the right pane it will display “**7 matches found**” at the bottom of the page but **only lists five (5)**.

On the left pane of the results page, you will see a City Filter and State Filter.

Counting the results for Amy Stewart

City Filter – 9

State Filter - 7

Unmask displays previous cities lived in the left results pane for subjects but no results in the right pane similar to Veripages.

It appears UnMask is redacting/hiding two of the results.

I tried one more people search site that I have had success Information.com. This site is related to Checkpeople.com.

After entering “Amy Stewart” I received nine hits which gave me the most of the three sites.

This time try **Radaris.com** - <https://radaris.com/p/Amy/Stewart/>

While using the above search URL – you will notice in the right website pane under Alaska you will see ten (10) results. When clicking the Alaska hyperlink – you will notice ten (10) results. Under different people name searches I have come across mixed results.

The **Spokeo.com** site appears to give proper result numbers with all the searches I have conducted.

I hope this helps locate additional information that may have been previously difficult to find or knowing additional information is out there that may not have been located before. ■

OFFLINE LIFE: DAPS REVISITED

By Michael Bazzell

In November of 2023, I published a blog post about my usage of Digital Audio Players (DAPs) as part of my offline life. I did not expect much response, as it falls outside of the typical topics which I usually discuss. However, it received more feedback than anything I had posted in many months. Most of the following is verbatim from that post, but I also added many new ideas about this space.

After returning from extensive travel, several people asked me about the gadgets I take. The usual list applies: Laptop, mobile device, etc. However, the most used item in my travel bag is a Digital Audio Player (DAP). I have never talked about these much, but they are a huge part of every day for me. I do not expect this post to resonate with this entire audience, but I want to share the many lessons I have learned over the years trying to chase audio perfection. I also just want to document my progress. I will relate this to privacy and security eventually, so please stick with me.

Some might equate a DAP with an iPod, but I hope to change that thinking by the end of this post. DAPs are much more than an MP3 player or a fitness device clipped onto your waist which holds a few albums. They offer a superior audio listening experience without the constant connection to (and distraction from) the internet and communication apps. My first DAP was a [Creative Zen](#) which contained a 60 GB 2.5" hard drive. At the time (2002), it almost held my entire music collection. It was heavy and bulky with an awful LCD screen, but it was magical. I later moved on to the [Zune](#) and iPod, but

neither scratched the itch. The storage space was always a limitation. Android phones with micro SD slots allowed me much more space, but the sound quality was lacking. The Sony Xperia line had decent audio, and I relied on those to possess my entire music collection until 2019.

In 2019, I discovered the [FiiO M7](#). This tiny \$100 DAP with micro SD slot was designed to provide better audio quality than a cell phone. It sounded amazing when paired with advanced In-Ear Monitors (IEMs) and I started to hear things in the music which I had never noticed before. I would later test the [FiiO M11S](#), [Hiby R6 III](#), and [iBasso 170x](#). I was constantly chasing audio bliss and fell hard for various marketing tricks, which will be debunked in a moment.

I should pause and state that I am a music fanatic, but I do not claim to be an 'audiophile'. I am extremely picky about my devices, configurations, and equalizer (EQ) settings, but I do not believe my setup is best for everyone. Music is a very personal choice, all the way from the genres, to the artists, to the production, to the desired output sound signatures. WARNING: I will share many things here which will infuriate some audiophiles.

I will upset the audio community right out of the gate. **I believe that most quality \$200+ DAPs SOUND almost the same.** Most people will not be able to tell the difference from the entry-level \$199 [Hiby M300](#) to the \$3000+ Astell&Kern line using their earbuds. Notice I said SOUND. Most DAPs are taking a digital music file and converting it to analog audio through a chip called a Digital Audio Converter (DAC). This

is a vital step to determine the audio quality we hear. As long as your chosen DAP has a dedicated and respectable DAC, the SOUND will be very close to any other DAP with a dedicated DAC.

This does not mean that the more expensive players do not offer any advantages, but this is where we can get into gimmicks. Cheaper players possess a single 1/8" (3.55mm) headphone jack while higher-end devices possess multiple jacks with 'balanced' output. Many people will say that the balanced output presents more "separation" or "sound stage", and I believe that is false. However, balanced output, amplification, and other features CAN be beneficial for some users. Let's breakdown the features.

Amplification: More expensive DAPs are usually heavier, bulkier, and offer longer battery life. This is because they also amplify the signal more than cheaper devices. If you are listening through sensitive IEMs or any other type of earbud, this simply will not matter. You will only need minor music volume to listen at a comfortable level through the unbalanced standard connection. If you will be using power-hungry 300-OHM over-the-ear style "can" headphones, you will absolutely need that power. This is where the style of headphone is important. Bigger cans need higher amplification. IEMs typically do not.

Balanced Output: Many people online will tell you that they hear a difference between a balanced output and an unbalanced output while using sensitive IEMs. I do not believe them. In fact, I have three self-proclaimed audiophile friends who insisted they could, but then failed an A/B test

when they could not see to which they were listening. Balanced output offers better amplification when you need to power large over-the-ear headphones. For those using anything in the ear, it should not matter. Stereo is stereo, and the marketing push of balanced output for most IEM listeners is unjustified.

DAC: Some cheap devices offer System-On-Chip (SOC) DACs which are combined with the other processing hardware of the device. These can be OK, but most are not. I can offer my own example. I had a Pixel 4A Android device with GrapheneOS as the operating system. Music within that device being output through the 1/8" headphone jack sounded fine until I applied EQ. Once I started emphasizing the bass levels, the DAC just couldn't take it. The sound was distorted. After plugging my headphones into a [FiiO KA1 USB-C DAC](#) on the same phone, the EQ'd music sounded great. This was an example of the difference a DAC (with better amplification) can make.

Most DAPs will offer either a Cirrus Logic or ESS DAC. My [FiiO M7](#) used the ES9018Q2C, which was the first time I realized what a good DAC sounded like. Again, many people will tell you they can hear a 'warmth' or 'sound-stage' within one better than the other. I am sure some rarities can, but most people cannot. Either is great. For me, it is more vital that my DAP possesses a dedicated DAC and is not relying on the system chip. The [Hiby M300](#) uses the CS43131 by Cirrus Logic.

Processor: Finally, this is something which will make a big difference. If the processor is weak, indexing music libraries and even playback can stall or fail. At a minimum, I believe a Snapdragon 6xx series is needed for any modern Android DAP. The 8xx series might appear smoother, but could be overkill for our needs. When you drop down to the 4xx series, indexing and playback feels sluggish and can ruin the experience. My brief time with the [iBasso 170x](#) was too slow.

Android: Many DAP fans prefer an Android-less operating system. These

are usually audio purists who do not want any other app, service, or 'bloat' to get in their way. They also want the best battery life possible. I respect that, but I prefer Android units because my desired music application requires Android. That application, discussed next, is also required for the EQ I like. Android devices also allow online streaming, but I never use it.

Poweramp: This is another area where audio enthusiasts are usually split. Every DAP will include a default music player. Some are better than others. I have tried them all, and tried to like them all, but I always come back to Poweramp. This \$6 Android app is an all-in-one music library, player, and equalizer. It also allows us access to Android hardware settings which we can use to tweak our output. I like the ability to modify the way my library is presented. Also, it always feels fluid, even with my 1.3TB music library. I believe the Poweramp EQ is better than the EQ options within many stock music apps. I offer many Poweramp optimizations in a moment.

Android Resampling: I believe this is mostly gimmick. Many people prefer 'bit-perfect' playback on their DAPs. This means that there is no extra resampling by Android in the path from audio file to delivery of sound through your headphones. Many Android devices will up-sample the final mix of audio from 44.1 KHz to 48.0 KHz in order to make sure that all streaming apps function properly for typical users. Some people say they hear a difference with this up-sampling, even though the human ear cannot detect those frequencies. I cannot hear a difference. I once thought I could until a blind test proved me wrong. The [Hiby M300](#) which I currently use offers a better implementation of this which up-samples the final output to 192KHz, and their stock app has no up-sampling at all. However, I do not think any of this matters to 99.9% of listeners.

Storage: This is a big one for me. I currently possess 10,232 albums consisting of 105,381 tracks, all properly encoded MP3s at 320 kbps. I need a lot of storage for all of that. I

currently use a [1.5 TB micro SD card](#), but most people should be able to get away with a much more affordable [1 TB card](#). Having every album with me at all times is amazing. My 19-year-old self with a wall of 1,500 CDs would not believe the future we have now.

Battery: This is important for me, but not the first thing I consider. I need a battery which will last all day, and I have yet to find a device which did not meet my needs.

Audio Files: The FLAC vs MP3 debate has been a hot topic for many years. FLAC has no audio loss and is the exact audio which was on the CD. MP3s are compressed, and technically lose some audio value (often in ranges the human ear cannot hear). I once insisted I could tell the difference between a lossless FLAC file and a properly-encoded 320 kbps MP3. I could play each and immediately hear the better option. When I had someone else administer the test, I could no longer tell a difference, or I guessed (being wrong 50% of the time).

I asked a music-producer friend with an amazing ear to prove me wrong. He is (was) a FLAC supporter. When blind tested, he could not tell a difference 50% of the time. Of the other half when he could tell the difference, he was wrong half the time. This is all anecdotal, but reflects my experiences. Any MP3s coded at 128 kbps or less sound awful, and most people can hear the difference. 160 kbps sound much better, but I can still tell they are compressed. 192 kbps sound great, and only occasionally can I hear an artifact which gives it away. I have yet to find anyone who could RELIABLY tell the difference between a 320 kbps MP3 and a lossless FLAC file in a blind test. Maybe a few 16-year-olds with amazing hearing can.

Hi-Res Audio / Sample Rates: High-resolution audio, also called high-definition audio or HD audio, applies to audio files with greater than 44.1 kHz sample rate or higher than 16-bit audio bit depth. It commonly refers to 96 or 192 kHz sample rates. However, 44.1 kHz/24-bit, 48 kHz/24-bit and 88.2

kHz/24-bit recordings also exist that are labeled HD Audio. To me, this is 100% placebo. Humans can detect sounds in a frequency range from about 20 Hz to 20 kHz. Infants can hear frequencies slightly higher than 20 kHz, but lose some high-frequency sensitivity as they mature. The upper limit in average adults is often 15–17 kHz.

44.1 KHz (16-bit) is the standard developed when CD's first arrived. It was chosen specifically for human hearing, since it would be an absolute ceiling of audible noise. Since then, 24-bit 'pure' recordings at 192 KHz arrived, often at over a GB per track, which promised us a whole new listening experience. We bought the new recordings of our favorite albums and claimed we heard a difference. When we truly did, it was due to remastering of the original tapes, not the higher resolution. Most DAPs support Hi-Res audio, but I believe those tracks are a waste of money. Anything at 44.1 KHz (16-bit) will suffice. I have yet to find anyone who could consistently pass an A/B test of a 44.1 KHz 16-bit file and the same recording at 192 KHz 24-bit.

Headphones: This is the most vital decision you can make if you want good audio. A pair of \$10 earbuds on a \$1,000 DAP will sound awful, and you are wasting your money. Also, a \$1,000 set of headphones connected to an old phone will sound equally as awful. Pairing appropriate headphones with your DAP is key to all of this. There are no perfect combinations for everyone, and anyone buying \$1,000 headphones will not care about anything I say here.

I believe quality IEMs are the most appropriate option for most readers, but I will also offer an over-the-ear recommendation in a moment. As stated previously, I have tried many devices and have fallen for many marketing tricks. Today, I have a simpler setup. I believe the new [Hiby M300](#) DAP (\$200) is more than enough for anyone wanting to get into the audiophile game. I pair mine with [FiiO's FH3 IEMs](#) (\$90). We should now discuss headphones. Picking the perfect pair is almost impossible, as there are over 1,000 headphones actively sold today. I

want to present some ways to eliminate inappropriate options.

Over-Ear vs. IEM: Your first decision should be whether you want a headphone which goes over your ear, such as a traditional set of "cans", or something which sits inside your ear, an IEM. In my experience, over-ear options present more of a wider sound while IEMs present more accuracy. IEMs tend to sound "Cleaner" and analytical while the cans present music more spaced out. I like both, but usually go with a high-quality IEM.

If you decide that an over-ear option is best for you, do you prefer an open-back or closed-back design? Open-back is typically preferred by audio purists, but there are issues with them. Open-back tend to present a more accurate musical experience because the sound is not bouncing around much. However, you can also hear everything else in the room (and other people can hear your music). Closed-back designs provide more noise isolation, but the music cannot escape the small area between your ear and the headphone. I prefer open-back while at home, but commuters should consider closed-back.

IEMs present even more confusion. Do you want dynamic drivers, balanced armatures, planars, or a hybrid? The following is a very basic summary of each.

Dynamic drivers are the most common type of earbud. These are very small round speakers which are similar to the speakers on a home stereo, only tiny. The vibrations of these drivers create the audio you hear. Your cheap earbuds likely possess a single dynamic driver for the entire audio spectrum. High-quality single-driver IEMs can sound great, but adding additional dynamic drivers helps a ton. This way, each driver can respond to a specific frequency range of audio. A 10mm driver can handle all the bass while a smaller speaker delivers treble and midrange. My first IEMs had three dynamic drivers.

Balanced armatures are even smaller and only deliver a specific range of

audio. These allow a portion of the music spectrum, such as bass, to be delivered via one armature while the treble is sent out another. This allows for a very detailed sound without distortion while listening to bass-heavy music.

I like both of these options, but not by themselves. This is why I typically prefer a hybrid of a dynamic driver (bass) and balanced armatures (midrange and treble). The FiiO FH3 previously mentioned is an example. It has one dynamic driver and two balanced armatures for clean, yet punchy, audio.

Planar headphones rely on magnets, and can have an incredibly detailed sound. This process was usually reserved for larger over-ear headphones, but there are now many companies making planar IEMs. If you want over-the-ear planar headphones which work well with a DAP, consider the [HIFIMAN HE400SE](#) (\$100). I have a pair I wear while at home to give my ears a break from internal IEMs. The sound is not as detailed, deep, and crisp, but the spacing of the soundstage is better than anything in the ear. They sound more like a performance than a CD. I currently do not own any planar IEMs as I am waiting to see what lands as the most preferred configuration.

Confused? I sure was. It took a lot of trial-and-error to settle on a few paces of hardware, and my preferences may be wildly different than yours. I recently convinced a family member to try better earbuds with a \$50 limit. I chose the [TRUTHEAR Zero RED Dual Dynamic Drivers](#) and she was thrilled. She was not aware of the punchy bass and crisp treble which was in her favorite music. I suspect she will soon migrate to the FiiO FH3s now that she has a new addiction.

I believe that any headphones over \$125 should be reserved for audio purists who have a very specific demand and already know what they want. The options presented here can stand up to most of the expensive offerings any day. Default settings on your DAP may be all you need in order to push your new

headphones, but I strongly encourage you to consider the following.

IEM Fit: When I first inserted my [FiiO FH3's](#), they sounded 'OK'. But then, I replaced the default earbud tips with a larger size and 'OK' turned into 'Holy...'. The fit is everything. You want a good seal which does not allow audio to leak. Find the tip which feels the best, then go up one size (multiple tips are included). I now feel the bass pound like I am at a concert and the highs are crisp.

I originally tried the more expensive [FiiO FH7's](#), but they felt weak to me. They were very accurate and 'analytical', but I wanted more warmth and overall depth. I think the cheaper [FH3s](#) are a sweet spot for a budget-friendly setup.

EQ: This is vital for me. I avoid non-android DAPs and stock music apps solely because of EQ. I believe Poweramp has an implementation of EQ which is superior to any stock music app. I encourage you to play with the EQ settings while listening to your favorite music. I typically leave the middle settings flat but turn up the left-side sliders (bass) and right-side (treble) until I have the desired result. I then work my way down each side so that my final result displays a 'V'. Only you can find your perfect place.

Hiby M300: I know I have mentioned this unit a lot, but I should explain why. Most DAPs I have tried were too heavy and bulky. They were great at home, but not ideal for travel. My original [FiiO M7](#) was an amazing size, but the screen was too small and the Android system is now far outdated. I tried the new [Sony NW-A306](#) (\$300) which was a great size, but the audio was quiet (due to restrictions on U.S. units) and the device was slow. The [Hiby M300](#) has checked all of the boxes for me. It is small but still has a 4" screen, great quality audio, decent amplification, Android 13, and it is smooth and snappy. I only have three complaints about this unit.

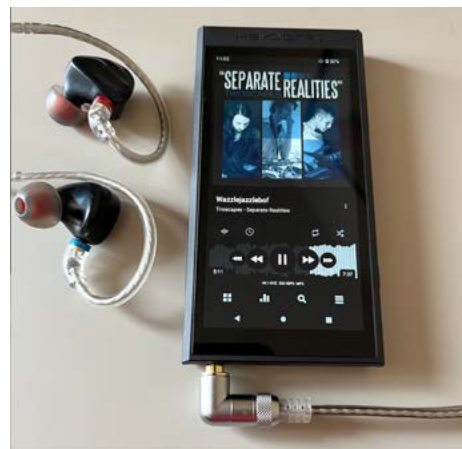
First, the master volume is not the same as the media volume. When you use the physical buttons to change

the volume, they change the master volume. That is fine (and preferred), but the Media volume might be too low to get what you want out of the device. I went into the Android sound settings and set the Media volume to '8'. I then change the master volume with buttons as needed. Consider the Media Volume to be the "gain".

Second, I experienced stuttering in my music when playing 320 kbps files using strong EQ through Poweramp. This was due to the system buffer not keeping up with the processing of my audio. I have experienced this on more powerful devices, and I offer my fix within the following Poweramp settings.

Third, and this was the only big one, Hiby does not respond to any support emails, so you are on your own. This is not a problem yet, but if you ever need to contact them about support or warranty issues, you will get no response. For \$200, and Amazon's generous return policy, I will take that gamble.

Note that the device has two screen protectors. One is meant to be removed before use and the other is more permanent. I took both off because the device always seemed to be covered in fingerprints and fine scratches. Without the protectors, the screen looks amazing. Below is an image of the M300 and FH3s.



If you end up trying Poweramp (they offer a free trial from their website or Google Play), here are the modifications I make to my settings.

Home Screen > 3 dots > List Options > disable unnecessary items / List compact

Artists > 3 dots > List Options > 1 line extra small

Artist > 3 dots > List Options > By year / Compact header / List Compact

Album > 3 dots > List Options > By track # / Compact Header / Show titles only / 1 line extra small

Genres > 3 dots > List Options > 1 line extra small

Genre > 3 dots > List Options > By Artist / Compact Header / List Compact

Album > 3 dots > List Options > By track # / Compact Header / Show titles only / 1 line extra small

Years > 3 dots > List Options > 1 line extra small

Year > 3 dots > List Options > By Artist / Compact Header / List Compact

Album > 3 dots > List Options > By track # / Compact Header / Show titles only / 1 line extra small

Settings > Look and Feel > Skin > Layout > Full Cover

Settings > Look and Feel > Skin > Font > Default

Settings > Look and Feel > Skin > Rounded Corners > Less rounded

Settings > Look and Feel > Skin > Seekbar Style > Static Seekbar

Settings > Look and Feel > Settings Theme > Dark

Settings > Look and Feel > Settings Font > Default

Settings > Look and Feel > Player UI > Album Art Animation > Disable

Settings > Look and Feel > Player UI > Chromecast > Disable

Settings > Look and Feel > Player UI

> Rating > Disable

Settings > Look and Feel > Lyrics > Lyrics Swipe Up > Disabled

Settings > Look and Feel > Lyrics > Lyrics Button > Disabled

Settings > Look and Feel > Lyrics > Scan LRC Files > Disabled

Settings > Look and Feel > Notifications > Navigate to the List > Enabled

Settings > Look and Feel > Notifications > Show Previous Track Action > Enabled

Settings > Look and Feel > Start at Library > Enabled

Settings > Audio > Crossfade... > Disable All

Settings > Audio > Equalizer > Auto Save > Disabled

Settings > Audio > Equalizer > Smooth ... > Disabled

Settings > Audio > Equalizer > Suggest... > Disabled

Settings > Background > Disable All

Settings > Library > -10/+10... > Disable

Settings > Library > Lists > Static Navbar > Enabled

Settings > Library > Lists > Bottom Buttons > Disabled

Settings > Library > Lists > List Item Click Action > Play and stay in the list

Settings > Library > Lists > Delete Action > Disabled

Settings > Library > Lists > Join Albums > Disabled

Settings > Library > Lists > Album Artist ... > Disabled

Settings > Library > Lists > Hide Unknown Album > Disabled

Settings > Library > Lists > Don't Ignore Articles For Sort > Enabled

Settings > Library > Scanner > Auto Scan > Disabled

Settings > Headset > Resume... > Disable all

Settings > Headset > Beep > Disabled

Settings > Send Errors > Disabled

If you use a lot of EQ, you may notice that the audio skips or lags. I fixed this on my [Hiby M300](#) with the following Poweramp settings. Note that I use the 'Hi-Res Output option'. The last two settings have no impact on the stuttering, I just prefer them for my listening (and audio collection).

Settings > Audio > Output > (Output Device) > Settings > Buffer Size > 100 ms

Settings > Audio > Output > (Output Device) > Settings > Buffer Size > Buffers > 4

Settings > Audio > Output > (Output Device) > Settings > Buffer Size > Post-fade 0

Settings > Audio > Output > (Output Device) > Settings > Sample Rate > 44.1 KHz

Settings > Audio > Output > (Output Device) > Settings > Sample Format > Auto

SUMMARY

OK, I know you are still wondering what this has to do with privacy and security. Most people listen to streamed music on their mobile devices. Not only are the devices always being tracked, but the streaming services are also monitoring what you like and when you like to hear it. I prefer to possess my own collection of audio files which do not require an internet connection. What happens when your favorite streaming service shuts down? What if you have no cellular access?

Local files will never let you down. For me, it is a matter of attention. If I listened to music on my phone while I hiked, I would constantly be tempted to check those pending emails or other communications. Today, my daily hikes do not involve a phone at all. I leave it at home. My DAP without any wireless connection and my library of audio is all I need. There are no distractions. There is no tracking. I am offline enjoying my day.

I have spent way too much time (and money) chasing the illusive perfect audio. When I was a kid, I had a Sony Mega-Bass Walkman. It was glorious. I went through hundreds of AA batteries flipping my 10 cassettes over and over. I only cared about the music and it probably sounded like crap compared to what we have today.

More recently, I wasted my time playing the same song twenty times in a row trying different cables, EQ, and outputs trying to squeak out one more drop of sub-bass or a crisper hi-hat instead of enjoying the album like I used to. Today, I give up on perfection. I know there will always be something better out there. So what? I now play full albums with my chosen DAP, IEMs, and EQ, and pretend I am a kid again. The audio I listen to now sounds better than it ever has, I just enjoy that and don't pay attention to all the hype. If you need a more powerful DAP to drive those 300-Ohm over-the-ear headphones, you know who you are. If you just want a great sound in your ears, I think you will be satisfied with this type of setup.

Disclosures: None of the companies mentioned provided me free products or payment for the reviews. Links are Amazon affiliate links. ■



Image: Ludovic Migneault

READER Q&A

By Michael Bazzell

We have not received many questions or letters since the hiatus of the magazine last year. If you would like to contribute a letter or question for the next issue, please email it to staff@unredactedmagazine.com. We look forward to your submissions. ■

UPDATES

By Michael Bazzell

A lot happens over the course of a year at IntelTechniques. The biggest change to impact readers is the switch from traditional print books to digital PDF downloads. We now offer our large OSINT and Privacy books as digital PDFs and introduced a new series of digital guides which include free updates as things change. More details (and bundle discounts) are available at <https://inteltechniques.com/books.html>. All purchases support the research required to keep our methods current. Please consider an updated guide for yourself, or as a gift to someone else. The following summarizes each product we offer.

OSINT Techniques, 10th Edition: 36 chapters | 260,000 words | 550 pages | 8.5" x 11" | \$30 - This textbook will serve as a reference guide for anyone who is responsible for the collection of online content. It is written in a hands-on style that encourages the reader to execute the tutorials while reading. The search techniques offered will inspire researchers to think outside the box when scouring the internet. Digital downloads include offline search tools, custom Linux scripts, and detailed report templates.

Extreme Privacy, 4th Edition: 22 chapters | 320,000 words | 517 pages | 8.5" x 11" | \$30 - This rewritten privacy manual is PROACTIVE. It is about starting over. It is the complete guide that I would give to any new client in an extreme situation. It leaves nothing out and provides explicit details of every step I take to make someone completely disappear, including legal documents and a chronological order of events. The information shared in this book is based on real experiences with my actual clients, and is unlike any content released in my other publications.

OSINT Techniques, Leaks, Breaches, & Logs: 9 chapters | 55,000 words | 162 pages | 8.5" x 11" | \$20 - This digital (PDF) supplement to OSINT Techniques delivers a much more thorough guide about data Leaks, Breaches, & Logs. It provides our entire playbook which we use to locate, acquire, clean, store, and query various online data collections valuable to our investigations. All expired and outdated methods were replaced with new techniques, and brand-new topics were introduced throughout. We also explain all daily, weekly, and monthly tasks required to maintain your data collection. **All updates are free and delivered digitally.**

Extreme Privacy, Mobile Devices: 16 chapters | 65,000 words | 152 pages | 8.5" x 11" | \$20 - This digital (PDF) supplement to Extreme Privacy delivers a much more thorough guide about mobile devices. It provides our entire playbook which we use for our clients when we need to acquire new hardware, configure a custom operating system, execute proper DNS filtering, enable push services, install applications, obtain anonymous cellular service, establish VoIP connectivity, program redundant data eSIMs, provide secure communications, apply VPN strategies, and troubleshoot the things which will go wrong. We also explain all maintenance and best practices for a new private and secure device. **All updates are free and delivered digitally.**

Extreme Privacy, macOS Devices: 10 chapters | 40,000 words | 111 pages | 8.5" x 11" | \$20 - This digital (PDF) supplement to Extreme Privacy delivers a much more thorough guide about macOS devices. It provides our entire playbook which we use for our clients when we need to sanitize previous Apple IDs; acquire new hardware; configure operating system

settings; execute a proper firewall; install applications without Apple ID; configure browsers, VPNs, and DNS; establish VoIP connectivity; create virtual machines; and generate custom scripts for daily usage. We also explain all maintenance and best practices for a new private and secure macOS device. Purchase includes custom macOS scripts and an import file to replicate all firewall rules. **All updates are free and delivered digitally.**

Extreme Privacy, Linux Devices: 10 chapters | 39,000 words | 101 pages | 8.5" x 11" | \$20 - This digital (PDF) supplement to Extreme Privacy delivers a much more thorough guide about Linux devices. It provides our entire playbook which we use for our clients when we need to acquire new hardware; configure operating system settings; execute proper DNS filtering; install applications securely; configure browsers and VPNs; establish VoIP connectivity; create virtual machines; and generate custom scripts for daily usage. We also explain all maintenance and best practices for a new private and secure Linux device. Purchase includes custom Linux scripts. **All updates are free and delivered digitally.**

Extreme Privacy, VPNs & Firewalls: 9 chapters | 34,000 words | 88 pages | 8.5" x 11" | \$20 - This digital (PDF) supplement to Extreme Privacy delivers a much more thorough guide about VPNs and firewalls. It provides our entire playbook which we use for our clients when we need to acquire new hardware; configure firewall settings; execute proper DNS filtering; configure web browsers; and establish VPN connectivity. We also explain all maintenance and best practices for a new private and secure firewall device. Purchase includes custom firewall configuration files. **All updates are free and delivered digitally.** ■

PRIVACY-THEMED PUZZLES

Puzzle

By **Danny Haas**

The following works as an escape (room) card. You have a key on the picture and you have to do some OSINT to figure out what the key means and then you can solve the puzzle.



Security Word Puzzle #4

Michael J. Ross

| | | | | |
|---|---|---|---|---|
| C | | | | H |
| | | L | | |
| | C | | N | |
| | | R | | |
| D | | | | S |

The objective of this puzzle is to discover the six five-letter words — all related to computer and network security — that fit in the above puzzle. Three of the words are horizontal and the other three are vertical, with overlap of some shared letters. Several letters have already been added to the puzzle to help you start. Here are the remaining letters needed to complete the puzzle:

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | M | N | O | P | R | S | S | S | S | T | U |
|---|---|---|---|---|---|---|---|---|---|---|---|---|

The solution to the previous security word puzzle consists of the following six words (three horizontal and three vertical): PATHS, ERASE, STEAL, PEERS, TRACE, SHELL.

FINAL THOUGHTS

By Michael Bazzell

I hope that this resurgence of UNREDACTED sparks new interest from contributors. If enough content was available, we would publish every month. Now YOU decide when the next issue arrives. I can't wait to see what you write.

MB ■

AFFILIATE LINKS

If you would like to support this free publication, please consider using the following affiliate links. If you plan to purchase any of the items below, or other items from the vendor (such as Amazon), the following links provide a small financial contribution to us without costing you anything extra. We see nothing about you or your order.

Extreme Privacy Book (Amazon): <https://amzn.to/3D6aiXp>

OSINT Book (Amazon): <https://amzn.to/3zoMZpZ>

Proton VPN VPN Service: https://go.getproton.me/aff_c?offer_id=26&aff_id=1519

Proton Mail Encrypted Email: https://go.getproton.me/aff_c?offer_id=7&aff_id=1519

Silent Pocket: <https://slnt.com/discount/IntelTechniques>

VARIANT DETECTED.

Websites and content.
For businesses who
respect privacy.

Be a variant.



Astropost

Astropost is the official design partner for this issue of UNREDACTED MAGAZINE. Need an ad designed for the magazine? Or a website that gives you results? We'll help you out!