

ISSUE 002

UNREDACTEDMAGAZINE.COM

JUN 2022

UNREDACTED

FUN WITH RADIO RECEIVERS

Monitoring distant radio
signals for fun and OSINT

OFFENSE & DEFENSE

Updates, anecdotes, stories,
questions, and letters from readers

THE LINUX LIFESTYLE

Transitioning to Pop!_OS as a
daily Linux operating system





**UNREDACTED
ISSUE 002**

Image: Jackson David

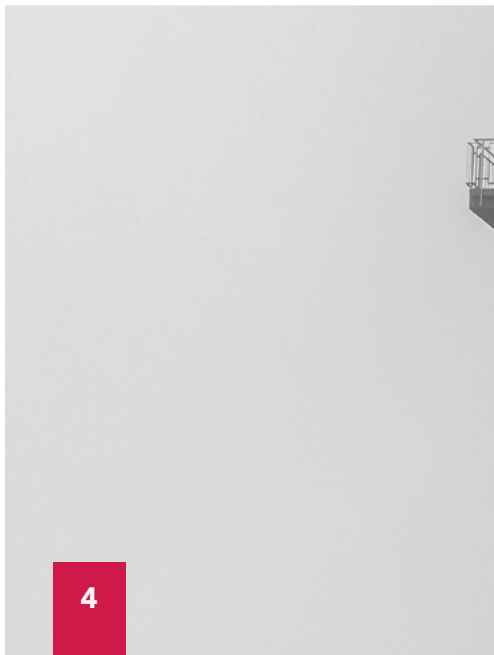
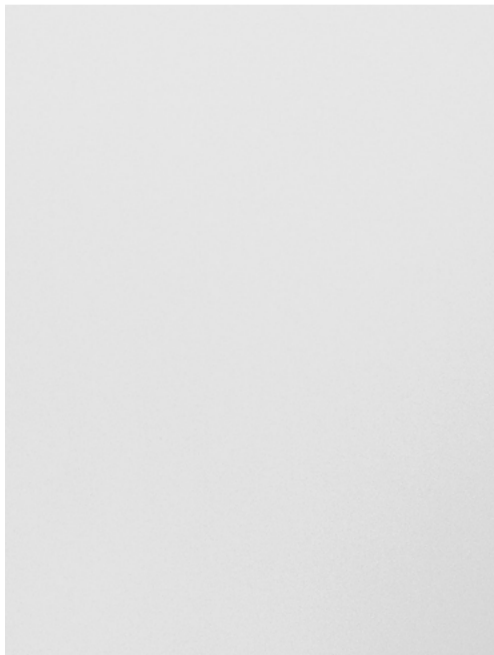
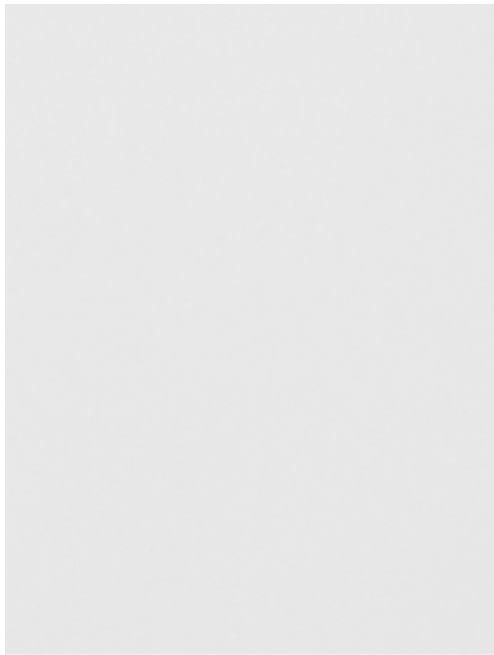
IN THIS ISSUE

- 5** From the Editor
- 6** Maintaining Multiple Google Voice Numbers
- 9** Bypassing Privacy Invasions of State Parks
- 10** Anonymous in Tijuana
- 12** The Linux Lifestyle: Switching to Pop!_OS
- 17** How Did Amazon's Cameras ID Me?
- 20** When 2FA Harms More Than Helps
- 21** Choosing the Right Wireless Provider
- 24** The OSINT Corner
- 26** Eulogy for the iPod Touch
- 27** The Home Address Dilemma and Form I-9
- 28** Fun With Radio Receivers
- 30** Reader Q&A
- 33** OSINT Book: Ubuntu Updates
- 34** Letters From Readers
- 36** Android Sanitization Package Names
- 37** My Secret Little Digital World
- 39** Wi-Fi Geolocation Concerns
- 41** Can Decentralized Identity Give You Greater Control of Your Online Identity?
- 43** Privacy-themed Puzzles
- 44** Final Thoughts
- 44** 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 [UNREDACTEDmagazine.com](https://unredactedmagazine.com). Contact details are also available at this site.

The contents of this publication are copyright © 2022 by UNREDACTEDmagazine.com, 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

Well, we made it to a second issue. I truly mean it when I say “Whew, what a relief”. Launching any new product is always a gamble. We estimate that over 30,000 copies of issue 001 were downloaded directly from our site within the first two weeks, and countless additional copies have been archived and shared all over the internet. Since we do not host any analytics on our site, this is a rough guess based on bandwidth usage of that otherwise minimal HTML-only website and the temporary access data within cPanel. I am thrilled with the response and interest, and excited to keep pushing new content.

This month’s layout will appear a bit different. Nick over at [Astropost](#) has volunteered to create a more polished and professional document, and we are grateful for the assist.

Many people have asked how we select articles for publication from those which have been submitted. In the first issue, we just published anything we found interesting. As more options are coming in, we must be more selective. I have three staff members who help me go through email and pluck out interesting items. All four of us have an equal say in what gets published. We assign a numerical score (1-10) to each entry and the highest scorers that month get published. We keep it simple for now. If your submission was not selected, please do not be offended. Consider polishing it up and re-submitting. FWIW, my first five

submissions to various hacker zines many years ago were all declined. The sixth attempt finally got through. Even worse, one of my articles for this issue did not make the cut (my staff can, and should, be brutally honest).

Several people submitted links to their various blog posts asking us to select one for the magazine. While I didn’t state it clearly before, we are looking for new and unique content. There is no need to re-publish something already available. We want this publication to contain new content unavailable anywhere else. We updated our submission guidelines to reflect this. This magazine is definitely a work in progress as we figure things out.

We had to make a few difficult decisions. Well, difficult for me at least. This month, the majority of the submissions were what we have since labeled “preaching to the choir”. These were mostly well-written articles about the reasons we all care about privacy. While these were great pieces, we decided we simply can’t publish all of them. Reading 100 pages about why we all agree that privacy is important doesn’t take us as far as reading about new techniques or unique situations. Therefore, we plan to limit each issue to only one article which fits this scope. That was hard for me because I wanted to simply publish everything we received, even if that meant a 40 GB PDF with 1,000 pages. My wise staff talked me away from that, and we will continue to focus on the submissions which teach us all something new.

We also saw a substantial increase in politically charged submissions. The balance was almost equal of the left blaming the right and the right blaming the left. Our desire is to keep this publication politically unbiased and eliminate anything which focuses solely on politics. There are plenty of other places online where you can scratch that itch.

Finally, we are introducing two new sections to each issue. The first is “The Linux Lifestyle” which will walk through an ideal Linux build using Pop!_OS which we can rely on every day for all of our computing needs. I will explain every tweak and customization which may motivate others to make the switch to Linux. As I find new applications useful to the privacy, security, and OSINT landscape, you will see it here first.

The second section is “Fun With Radio Receivers”, where I discuss the many ways to monitor radio signals for hobby or OSINT. Both of these sections will appear every month and cover many details of the ever-expanding realm. Both categories were in my head when I began considering this publication, but I wanted to get the first issue out before committing to this task. User submissions for each are welcome.

Again, thank you for being here. We have a lot to do, but I look forward to the journey.

~MB

MAINTAINING MULTIPLE GOOGLE VOICE NUMBERS

By Michael Bazzell

Theoretically, assume that I have dozens, if not hundreds, of Google Voice numbers. Maybe I have taught live OSINT courses since 1999 and part of every course was a live demo for creating a new Google Voice number while using hotel phone lines and library fax machines as verification numbers. Also assume that I have maintained all of those numbers over the years and I can use any of them when needed. Again, this is all theoretical, as this would violate Google's terms of service. Now, assume I have a conundrum. How do I keep them organized and active?

There are a few concerns if you start to possess multiple Google Voice numbers. The first is suspension of the account. If you ever log in from a suspicious network or device, Google is known to suspend your account until you provide proof of your identity. Since you probably created the account in an alias name, verification could be difficult, if not impossible. Next, you risk loss of the number due to lack of use. Google states:

Google may reclaim your Google Voice number (if you have one) if you have not placed or answered calls, or sent or opened text messages for a period of 3 months. We will

not reclaim numbers that have been ported into Google Voice or made permanent.

This is not completely accurate. If you own a Google Voice number which was not used within 90 days, you have probably received a warning from Google telling you to make calls or send text messages to keep the number active. While Google indicates incoming calls and text messages reset the clock, they do not. I have tested this thoroughly. I have a Google Voice number which receives a spam call every day and at least one spam message every week. If I do not place outgoing calls or texts within 90 days, I get the dreaded email telling me I must use the number or lose it. Therefore, incoming communication does not qualify as active use of the account.

Next, there is the issue of organization of all of these numbers. It is one thing to store them all within your password manager (I do), but how should we access each number? Is clearing browser cache enough to eliminate all evidence of usage? Finally, there is a concern about contamination. If I download the Google Voice app onto my mobile device and log in and out of numerous accounts, I just told Google that they all belong to me. Let's address each of these issues while I present my desired solution.

The short answer here is a dedicated Firefox browser, only used for Google Voice, with isolated containers for each account. The long answer is more complicated.

On my primary Linux computer, I have standard Firefox as my daily browser. I have also installed Firefox Beta as an isolated browser which is never used for anything but Google accounts. Before attempting any login, I installed the Firefox Multi-Account Containers add-on and created a new container for each Google account. I labeled the container as the Google Voice number associated with the account. I also set the Google Voice login page as the default home page for every container. I installed uBlock Origin with the default settings to block some of Google's data collection. Once I configured, let's say all 112 numbers, I was ready to start attaching the accounts.

One must be careful here. If you start logging into numerous accounts from the same IP address and browser characteristics, this will result in an account suspension. Therefore, take it slow. If you have previously accessed a Google account from behind a VPN, there is little harm in repeating this process. When I set up my system, I logged into only two accounts per day within the specified containers. I then waited until the next day when my

home firewall had issued me a new VPN IP address to enter two more.

I had a couple of difficult accounts which did not allow me to log in behind a VPN due to “suspicious” behavior. A trip to a library allowed me to use their public Wi-Fi without a VPN to make Google less suspicious of my login attempt. It took some time, but today I have every Google Voice account credentialed within one sole-use browser isolated within a single container for each account. In the bottom right-hand corner of this page is an image showing an example with false data.

One huge benefit to this is that you can elect to allow your browser to store all of your session data and never wipe it out. On my primary Firefox browser, I have it set to wipe everything out every time it is closed. This keeps my sessions clean without additional tracking by websites. With this new protocol, we want the opposite. I do NOT want my browser to wipe out anything ever. I want it to keep all session cookies and cache every time it is closed, so I make sure that is how my settings are configured.

This way, even if you have not accessed a specific Google account for a long time, opening that container should present you with your account already logged in. If you have been logged out due to time, logging in tells Google that the device is trusted because of the stored data. It bypasses many of Google’s security checks since the account has been accessed on this device in the past. This is much different than logging into a Google account from a clean machine, which always causes scrutiny.

If desired, you could replicate this with a secondary Firefox app on your mobile device, such as Firefox Beta or Nightly. However, I do not recommend this for two reasons. First, Google is known to flag multiple accounts connecting from a mobile device with the same IP address within a short amount of time, even through a browser. Second, the task of creating profiles and entering the data is a burden. You could try to

copy over cache from one browser to another, but that could look more suspicious. For me, having them all within a browser on my laptop is sufficient. I never recommend installing any Google product, especially the Voice app, onto any mobile device. I only access these numbers through a browser container.

Is this a perfect privacy solution? No. Google can still use browser fingerprinting to possibly determine that these accounts are being accessed on the same machine. However, Google probably has enough data at this point to do this anyway. I am sure that something within my usage over the past decade could tell their systems that these accounts could all belong to the same person.

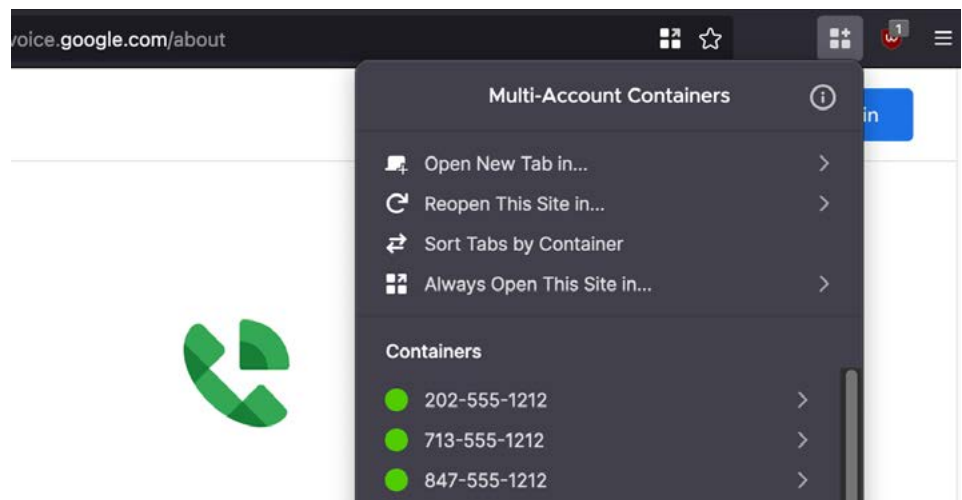
I never use these for anything sensitive or tied to an alias which must be isolated from my real life. I rely on MySudo for that.

Now comes the issue of number recycling. Just because the accounts have an active (but dormant) credentialed login, it does not prevent Google from trying to terminate your accounts for lack of usage. I have every Google Voice account set up to forward email, voicemail, and text messages to a unique SimpleLogin masked forwarding account. This adds another layer of similarity to each account, but I am fine with that. The emails all forward to a dedicated email account which is part of my paid ProtonMail package. About once a week, I get the email from Google saying they will reclaim

my number in 30 days if it is not used. I open the Firefox Beta browser, open the container for that number, and immediately see my account. I make a return call to the last spammer that called me and then send a text message response to the latest scam message. That meets the requirement to keep the account active another 90 days.

Is this as simple as I would like? No. However, it is not that difficult. I don’t need to log into the account because the session credentialing has been saved in the container and Google does not see that activity as suspicious because I am connecting from a “trusted” machine. This all takes some time to create, but the final product is easy to use. I can open a container with a specific number I want to use and make a call within seconds.

It is important to never open all containers at once or any containers which you do not need to use. If you do this, Google sees that activity and their systems might suspend all of your accounts. I make sure to close each tab when I am done. That way, when I open the browser next time, there are no active sessions loaded. I only see the Google Voice login page from a non-container window. As long as you do not execute a container, Google is not being notified that you opened the browser for any specific account. Your mileage may vary here. Please only take this as one option of many. Please send in any modifications you find useful. ■





The World's Only All-in-One Privacy App



Sudos act as digital firewalls to eliminate data trails.



Call, Text, Email, Browse, Shop and Pay
Privately and Securely



Create digital identities,
or **Sudos**, for different situations.



Research
Jackie Russell

jackierussell@sudomail.com



Travel
Jackie Russell

jackierussell02@sudomail.com



House Hunting
Jackie Russell

jackierussell03@sudomail.com

Sign up without an email, phone number or password | MySudo.com/bazzell



BYPASSING PRIVACY INVASIONS OF STATE PARKS

By Anonymous

I live by a beautiful state park which requires a fee for entry. Maybe I have said too much. For a while I was buying a daily pass with cash when I arrived at a self-service kiosk. Since I go so much, I decided to buy an annual pass this year to save money and support the institution. I grabbed \$50 in cash and went to the main office to buy my sticker. There was someone in front of me and watching his experience turned out to be very helpful in my demand for privacy. He was also purchasing a yearly pass. The worker demanded his driver's license, vehicle registration card, email address, and cell phone number. Wow. That seemed surprising for a cash purchase. He handed over his license and the worker typed in various details from it. She then laid it on a small flat scanner and collected a photocopy of the front including all details and his picture. He walked away with his sticker. Then it was my turn.

When I asked for an annual pass I was asked for my license. I told her I didn't bring it with me and she said it was mandatory. She began an entry with my details to "get me in the system" and asked my name. I provided my true first and middle name which she probably assumed was first and last. Since this was technically a government entity I didn't want to lie. She then asked if I knew my license number. I didn't but thought I would try something else. I said "my number is" and then I provided a VoIP telephone number I own. I didn't say it was my DL, I only said it was my number. Still being somewhat "honest".

Then something surprised me. She said that the number I gave was not a

valid license number. What state was she checking? Does she have access to the local DMV? Does she have access to EVERY DMV? This seemed weird so I told her I would come back. Apparently I was not prepared. I couldn't believe I would need to provide so much detail and allow an image of me (and my DL) to be insecurely stored until a data leak exposed it to the world. I just wanted a park pass!

While at home I did some research. I knew I needed a valid driver's license number and vehicle plate number. I knew I didn't want my real information on the record, that I didn't want them to scan my license, and that I wanted to be allowed to use whatever pass I bought without scrutiny. I had provided only my first and middle name which are both very common. I needed a DL number which would pass whatever verification check they were doing. I went to the Data Design Group website at ddginc-usa.com. I clicked the Florida Driver's License Generator in the tools section. I entered my first name, no middle initial, and my middle name within the last name field. I entered my real day and month of birth but a year of 1901. This generated a license number similar to S530-420-01-001-0. I was ready to try the purchase again but with more confidence.

I arrived at the state park the next day and saw a different employee working. I walked up and said that I had talked with Katie yesterday about buying a park pass but I didn't have all of the details she needed, but I was back to complete the purchase. I provided my first and middle name but they could not find me in the system. It seems Katie did not save what she entered. I was asked for my license but

told her that I had lost it and Katie said to just bring in the number (I did lose my license when I was 17). The worker proceeded to complete a digital form on her computer and asked for my name, address, email address, and cell phone number. My first name, middle name, CMRA address, burner email, and MySudo VoIP number passed all scrutiny. I was then asked for my driver's license number. I said "Can I read you a Florida number?" and she typed the number in. Notice I didn't say here is "MY" license number. Only if I could read "A" license number. Since the number I created would be for a person 121 years of age, I felt safe with giving that out. Her system accepted the number and we moved on.

I paid the \$50 and she said that she needed my license plate to be printed on the pass. I was ready for this. I said "OK, the digits in my plate are G76E01". This was true but I accidentally reversed two of the numbers. If a ranger ever compares my true plate to the sticker it will look like a typo. This way my actual registration is not in their system for abuse or breach/leak. I was issued my sticker and I left. There was no fraud. I technically did not ever lie. I paid the money. I supported the park. I also refrained from providing my full unique name, an image of my face, and a unique identifier which could be used for identity theft. I used a sticker shield for the pass which allows me to remove it from my windshield whenever I leave the park. When did it become this hard to buy a park pass with cash? ■



ANONYMOUS IN TIJUANA

By AnoninTJ

As a longtime listener of the Privacy, Security, & OSINT Show, it's kinda obvious that there'd be a significant portion of the readership of this new publication who'd be interested in anonymity. If you're in that category or just want a good read, allow me to tell you about some of my experiences in Tijuana, Mexico. A note before we continue. Nothing you are about to read should be considered as legal and/or professional advice. Or maybe even taken seriously.

Tijuana is a large, third world city in a large third world country. It and the country's borders are back to back with

the border of the United States and as such offer interesting possibilities as far as privacy and anonymity are concerned. Before we get into the weeds, so to speak, one of the more interesting aspects of the city and the country in general is that corruption is rampant. As in omnipresent. It's everywhere and anyone who has the opportunity participates. Depending on just how socially and/or legally unacceptable you want to be, a discreetly and well placed 500 peso note will turn most heads for the amount of time necessary to not notice something.

I have personally experienced walking through the border checkpoint and into Mexico at the Otay border

crossing without comment or questions or having to produce documentation. And I look like a gringo. This is not an everyday occurrence however. If you don't have or can't get the required legal documents and just have to enter the country, try the Otay crossing, and that discreetly and well-placed note of legal tender mentioned above could very well get you in. Or you might be able to just waltz right in like you own the place. Leaving, though, could be another thing entirely, so think things through. Do the OSINT.

Before arriving, it's good to know some Spanish. Many years ago when I crossed the border for the first time, I knew two words of the local language.

Si and no. The intervening years have been an interesting survival and learning experience. In Tijuana itself there's a significant portion of the population that understands and can speak at least a few common words of English. Google Translate can be quite useful. Being open, friendly and non-assuming can be, and are, valuable personality traits.

Due to being right next door to San Diego, a cross section of the population is quite diverse. Whatever you look like, there's a good chance that there's others here who look like you. It's best to dress like and carry the accoutrements of the common person. The people here are survivalists. If you look like you're an opportunity, you'll be considered as such. It's good to arrive with a single backpack that's as small as possible and contains just the essentials. Secure anything you can't live without discreetly to your person. Anything else, and I mean *anything*, that becomes necessary can be acquired here.

Please do not arrive in a motor vehicle. This only increases the necessary legal entry hassles and the effort required to get into the country. Also, traffic here can approach nightmare status. Driving here is an art form as opposed to the science of driving in the States. You've been warned. What follows assumes that you intend to be here for an extended and/or indefinite period of time.

Whether you land in El Centro or Otay, move beyond there as soon as possible. 5Y10 offers discretion and non-touristy opportunities and many local transportation services have routes from either of those landing areas to 5Y10. Lower-end places will often forgo an ID requirement or look the other way for a few additional pesos.

It's good to bring a carrier unlocked, GSM compatible smartphone with you. Find an Oxxo store (they're omnipresent) or any place displaying a Telcel sign, and get a Telcel SIM card and a couple hundred pesos of air time. No ID is required, just pesos. Google

Maps, Translate and a good search engine (Startpage) will be invaluable. If you're a Reddit user, the r/Tijuana subreddit can offer helpful advice and interesting reading, often in English.

Dr. Simi is an omnipresent pharmacy chain with outlets throughout Tijuana and Mexico in general. Find one and acquire Loperamida, an anti-diarrhea OTC med, and Paracetamol for minor head and body aches. No ID or prescription required. A supply of each should not set you back more than 50 or 60 pesos. Not being bothered by aches, pains or the need to defecate every ten minutes will do a lot to ease your transition into third world society and culture.

Find a low-end place to hunker down and get busy searching for cheaper digs. If you've arrived in Tijuana without official documentation, listen up. While in the city itself, I've never been stopped by anyone who presumed themselves to be in a position of authority and demanded that I produce ID or travel documentation. And I've been here a while.

If you intend to move further from and beyond the city itself, this can become a problem. A quite expensive and inconvenient problem quite quickly. Hitchhiking/walking is a travel option to possibly circumvent authority. Possibly. Consider moving beyond Tijuana very carefully. Do the OSINT.

Gettin' low on cash?? At the time of this writing, there's a Bitcoin ATM somewhere (do the OSINT) in Tijuana that both sells and buys Bitcoin anonymously for U.S. dollars. With U.S. dollars it's possible to anonymously exchange them for MX pesos throughout the city. If you need or want to work, there are gig type opportunities that don't require documentation. You'll find what you're looking for. Beggars and scammers are quite common. If you go that route, you'll have lots of competition.

Oh, in Tijuana, cash is king. You don't need, and I wouldn't recommend, bringing credit or debit cards. Especially if you want to be anonymous. Use

Mexican pesos. There might be places that accept Bitcoin, although I've not encountered them. Haven't really looked though.

Pro tip: learn as much Spanish as fast as possible. In fact, beyond providing safe drinking water, food and safe shelter for yourself, learning the local dialect could be one of your highest priorities. About safe drinking water: do not drink tap water, no matter where you are, unless there is no other option. Bottled drinking water is readily available and inexpensive. As well, alkaline water (agua alkalina) is available. Look for it. You could also bring a Grayl Geopress and a couple extra cartridge replacements with you. This could be considered essential travel gear.

So, you are resourceful and can provide for yourself without being a burden or a nuisance. Congratulations and "Bienvenido a Mèxico"! Stay curious, ask questions, be friendly and non-threatening. Be anonymous, safe and well. ■



THE LINUX LIFESTYLE: SWITCHING TO POP!_OS

By Michael Bazzell

The Linux Lifestyle is a new monthly column all about Linux. From new useful apps to working through Linux frustrations, this section aims to introduce others to a more secure operating system.

Every other April presents the perfect opportunity to refresh my laptop and desktop computers. In April of even years (2020, 2022, etc.), we see the release of a new Long Term Support (LTS) version of Ubuntu Linux. This April we were given Ubuntu 22.04, which includes support via software updates for at least five years. I always take this opportunity to completely reinstall the operating system and all applications. This removes any outdated or undesired data from applications which have since been removed and various caches which have begun to clutter my system. It also allows me to jump right into the latest LTS release with a clean slate and no software conflicts or less than optimal configurations. It is the equivalent to reformatting a Windows or Mac machine when it gets slow, but a bit more tied to a schedule instead of a specific need. As a nerd, I look forward to April every other year.

I now rely on two Linux systems. My desktop is always at my home and is the system which I use over 90% of the time. The desktop format allows me to easily add more internal storage, RAM, or peripherals. It also pushes me to be more intentional about my computer usage. I now avoid taking the laptop from my home office into the living area, as it encouraged me to always do “one more thing” while watching a movie or spending time which should be away from a computer screen. Having a desktop helps me isolate work and life more than a laptop always by my side.

The desktop also allows me to really “turn it off” when I am finished with work, and gives me a sense of walking away from the office. Closing a laptop lid does not give that same feeling of closure for the day. I now reserve the laptop for travel, which has been

minimal over the last two years. Both devices are clones of each other with the exact same OS, apps, and data. I synchronize documents weekly, and both contain fully encrypted discs. My desktop also does not possess a camera or internal microphone, which eliminates any accidental broadcasts. I find this comforting. I also rely on ethernet for my network access, and never need Wi-Fi enabled on the desktop device. Win. Win. Win.

Typically, I would just download the latest Ubuntu LTS ISO file, wipe out my machine, and reconfigure everything, but this year is different. Instead, I am taking the plunge and using Pop!_OS as my operating system on both of my devices. Pop!_OS is based on Ubuntu, and is also on the 22.04 LTS release. It is maintained by System76, who also makes the computers I use every day, but is ideal for any hardware which

supports Ubuntu. The following are my reasons for the switch.

- Pop!_OS looks more polished and professional. All of these tweaks could be made manually to Ubuntu, but I prefer the overall “feel” of Pop!_OS.
- Pop!_OS is specifically designed with System76 hardware in mind. Since I use their computers exclusively, it makes sense to go this route. There is no need to find Wi-Fi drivers or worry about video card conflicts.
- Ubuntu 22.04 forces Snap as a package manager on users. This can take up more space for each installed application and software execution times can seem slow. If you reboot Ubuntu 22.04 and launch Firefox (now a Snap package), you will see what I mean. I prefer APT (Advanced Packaging Tool) for Firefox, which is used by Pop!_OS. One could remove Snap completely from Ubuntu, but I prefer to simply use Pop!_OS.
- Pop!_OS has a great implementation of tiling by default. This allows your windows to automatically resize to fit your screen. I find it better than other third-party options, and even the macOS split screen ability. You could replicate this within Ubuntu, but I find the default behavior in Pop!_OS to work best.
- Pop!_OS presents a more minimal default installation with less applications (and less bloat) than Ubuntu. I appreciate the responsibility to install what I need.
- The Pop!_OS software shop is based on Flatpak instead of the Ubuntu Snap option. I find this better suited to my needs (and the needs of my clients).
- Pop!_OS enables encryption by default, and a recovery partition is included in case something bad happens. The existing operating system can be repaired or

reinstalled from the recovery mode. You can perform a fresh install without losing any user data.

When rebuilding my machines, I began with the desktop. This way I could work from my Lemur laptop while I configured everything for daily use on the desktop. After the desktop was functional, I could wipe out the laptop. My chosen desktop is a System76 Thelio due to its small form factor and expandable storage (four 2.5” SATA drives and M.2 NVMe port). A decent configuration is less than \$2,000 and is plenty of power for my needs. If you are a heavy gamer or you render long 4K videos every day, you will need more power than I do. Always consider your own specifications carefully before any purchase, and understand each option.

In the interest of full disclosure, System76 was a sponsor of my podcast in 2018 and is currently a sponsor of this magazine. However, I have purchased multiple System76 machines for myself and my clients, and I have promoted them for years within my books at no cost to them. This is because I prefer their systems over any other Linux-based computer providers for several reasons.

First, they offer machines which have potentially invasive processor software disabled before delivery. Specifically, they apply a version of Intel Management Engine (IME) which does not have remote management parts enabled. The latest Intel processors require IME to function, but System76 eliminates the most invasive features. Some laptops have IME disabled completely. Do your homework and identify your threat model. I always prefer Intel processors since AMD’s equivalent, PSP, cannot be easily disabled.

Second, many laptop models include a completely open-source BIOS called coreboot which allows a faster boot time within a more secure environment. Look for this feature in the specifications if it is important to you. I speak more about these options on podcast episode 264.

Third, System76 devices are created specifically for use with Linux, which is important to me. I know that all necessary drivers will be included and any hardware options are ready for Linux. I don’t worry about troubleshooting Wi-Fi, audio, or video issues when I install a new Linux OS. Finally, support is available anytime I have issues. As I was writing this, I placed an order for a new desktop device. I received live updates to the build status, and I sent a question about IME being disabled. I received a response within 30 minutes. All of these features are a requirement for my personal computers, and those of my clients.

Installing Pop!_OS is no different than most other Linux builds. Download the ISO from their website (pop.system76.com), flash it to a USB drive using a program such as Etcher, insert it into the computer, boot to the drive, and begin the installation. If ordering through System76, you can select Pop!_OS as the included OS. During installation, select “Try or install Pop!_OS”, select your language, perform a clean install, choose your disk, provide your details, and restart the machine. Upon boot, customize your appearance options and you finally possess a Pop!_OS system ready to go.

Now the fun begins. I have a very specific protocol when I reinstall an operating system. I don’t play around with anything until I have a few things in place. The first is to apply all updates. This is easiest through the Pop!_Shop. This will install pending system, application, and driver updates.

Next is optional DNS configuration. In the past, I have relied on OpenSnitch to block undesired outgoing connections from my Linux laptop (after using Little Snitch on macOS for many years). However, I no longer recommend this. OpenSnitch has been quite buggy and can severely slow down your system. It can also be quite an annoyance. Furthermore, Linux does not share data about your usage in the same way macOS and Windows does. Since I rely on open-source applications which have been vetted by our community,

I simply don't have a strong need for OpenSnitch to block any suspicious connections. Instead, I now rely on NextDNS when necessary. I explain this in great detail within my book *Extreme Privacy*, but let's go over the basics.

NextDNS (nextdns.io) conducts the DNS queries required in order to navigate your internet traffic, but it also includes filtering options. First, create a new free account at my.nextdns.io/signup. Any masked email service should be accepted, and no payment source is required. I used an alias name. The free tier allows 300,000 monthly queries at no cost. After registration, you should be taken to your user portal which should display your unique DNS addresses, similar to "12a345.dns.nextdns.io". You can now use this address, or the other configuration options, to use their DNS service and filtering options within Firefox or Android devices. Within Linux, we must configure a few more steps. In Terminal, I entered the following.

```
sh -c "$(curl -sL https://nextdns.io/install)"
```

This walked me through the installation process. When prompted for my Configuration ID, I provided the unique identifier from NextDNS, 12a345. I answered "Y" to all questions with the exception of "Setup as router?", to which I answered "N". I then launched the service with the following command in Terminal.

nextdns start

The service was then running on my computer, and NextDNS was providing the DNS query service. I can go back to the NextDNS portal and make sure logging is enabled in the settings menu. If it is, I can click on the "Logs" tab and monitor the connections being sent from the computer. In my scenario, I saw nothing. This is because my Pop!_OS operating system is not calling home about my usage. If I were on a macOS or Windows system, it would be full of calls back to those companies sharing data about anything you do. When I opened the Pop!_Shop and checked for updates, I saw a single connection attempt to apt.pop-os.

org, as expected. This is how I know that nothing suspicious is happening behind my back. I can also enable "Blocklists" under the Privacy tab which will block known annoyances such as ads, trackers, and analytics. I prefer the Energized Ultimate blocklist.

You can also block any individual outgoing connection you desire. If you find that an installed application is sending telemetry to their servers about your usage, you can add that domain to the "Denylist" in your NextDNS portal. There are many options here to explore.

Your computer should now be blocking connections as you desire. I rebooted my machine and watched the log within NextDNS. The NextDNS utility launched on its own, hidden in the background, within my Linux system, and I saw four connections. Two were to Pop!_OS servers checking for updates, and two were to Canonical servers, the creator of Ubuntu (the backbone of Pop!_OS), also checking for updates. I do not find either intrusive. If this had been a macOS operating system, I would have seen dozens of connections sending various data to Apple and iCloud servers, which would be stored forever and associated to the Apple ID and serial number of my device. Linux does not do this.

Your computer should now be updated and blocking undesired outgoing connections. Remember that the free tier allows 300,000 queries per month. If you find yourself exceeding that, you might consider a paid tier. You also might consider whether you need DNS filtering at all. I think you will find that Pop!_OS is not sending your data to servers in the way that Apple and Microsoft do. If you are satisfied that nothing on your system is sending malicious data to third parties, you may want to remove NextDNS. Simply enter the previous installation command and choose "r" to remove it completely, if desired.

What do I do? I leave the NextDNS utility installed and enabled. I allow NextDNS to serve as my DNS querying and filtering service. If I ever need

to disable it, typing the following command within Terminal turns it off.

nextdns stop

When I install a new application, I re-enable the NextDNS logging capability within their portal and monitor the logs to make sure there is nothing which needs manually blocked. Once I am satisfied, I disable logging within the NextDNS portal. I have yet to find an application I use in Linux which needs to be blocked, but I am picky about my connections. You may feel different. You might require a software application which is sending telemetry to various servers. If you do, then you should keep this option active. If you see nothing suspicious, then you might consider disabling it and using another DNS provider. There is no harm in allowing NextDNS to always run in the background. Since I have a home firewall running pfSense handling my DNS traffic, I have less need for NextDNS on the machine itself, but I like the filtering of various online annoyances. Every situation is unique, and you should know your options. Play with this and see if it is appropriate for your setup.

In summary, NextDNS is running in the background of my machine at all times. It conducts my DNS queries and filters many unwanted connections as I browse the internet. It is also there to investigate any suspicious activity from within applications.

Pop!_OS includes the non-Snap version of Firefox. Ubuntu forces Snap for the installation and their app store, but Pop!_OS does not include Snap at all unless desired. I use Firefox as my daily browser, but I always make a few adjustments. The first is to install the add-ons uBlock Origin and Firefox Multi-Account Containers. I explain more about each in my *Extreme Privacy* book, and most readers are probably already familiar with them. Next, I tweak the default Firefox privacy settings with the following.

- Click on the menu in the upper right and select "Settings".

- In the "General" options, uncheck "Recommend extensions as you browse" and "Recommend features as you browse". This prevents some internet usage information from being sent to Firefox.
- In the Home options, change "Homepage and new windows" and "New tabs" to "Blank page". This prevents Firefox from loading their own sites in new tabs.
- Disable all Firefox Home options.
- In the Search options, change the default search engine to DuckDuckGo and uncheck all options under "Provide search suggestions". This prevents queries from going directly to Google, and blocks the Google API from offering search suggestions.
- Click the "Privacy & Security" menu option and select "Strict" protection.
- Check the box titled "Delete cookies and site data when Firefox is closed".
- Uncheck the box titled "Show alerts about passwords for breached websites".
- Uncheck the box titled "Suggest and generate strong passwords".
- Uncheck the box titled "Autofill logins and passwords".
- Uncheck the box titled "Ask to save logins and passwords for websites".
- Change the History setting to "Firefox will use custom settings for history".
- Uncheck "Remember browsing and download history" and "Remember search and form history".
- Check the box titled "Clear history when Firefox closes". Do not check the box titled "Always use private browsing mode", as this will break Firefox Containers.
- Uncheck "Browsing history" from the "Address Bar" menu.
- In the Permissions menu, click "Settings" next to Location, Camera, Microphone, and Notifications. Check the box titled "Block new requests..." on each of these options.
- Uncheck all options under "Firefox Data Collection and Use".
- Uncheck all options under "Deceptive Content and Dangerous Software Protection". This will prevent Firefox from sharing potential malicious site visits with third-party services.
- Select "Enable HTTPS-Only Mode in all windows".

These are what I consider the "staples" as far as browser hardening is concerned. In future articles, I plan to dig deeper into ways we can further protect our online activity. There are many opinions on the perfect browser setup, so I will stop here for now. There is much more to discuss.

Next, I installed my desired applications through the Pop!_Shop. For me, this included KeePassXC, Signal, Wire, Element, Atom, Standard Notes, Electrum, Kodi, Transmission, VLC, GIMP, Tor Browser, FreeFileSync, Audacity, Handbrake, Calibre, and others. Pop!_Shop will notify me when there are updates to these apps, or anything installed via APT. Some desired apps will not be present within this shop. There will always be scenarios where we need to install software manually. One example is VeraCrypt. I installed it by downloading the most recent Ubuntu GUI ".deb" file from the official website, right-clicking it, choosing "Open with Eddy", and clicking "Install" within the Eddy application. Eddy is a Debian package installer included with Pop!_OS. Any time you download an installable ".deb" file, Eddy can install it to your system properly.

If you desire a beta version of Firefox, as previously explained useful with Google Voice account isolation, you only need to install a second version. Pop!_OS makes this easy. If you open the Pop!_Shop application and search

Firefox, you should see two options. One is already installed by default, which I use as my daily browser. The second option, which displays an "Install" button next to it, has additional options. Click the entry (but not the install button) to open the menu. Change the drop-down menu from "flathub (flatpak)" to "flathub-beta-flatpak" and click "Install". If the drop-down is missing, just install this second version. You should now see two versions of Firefox in your Application menu. They can run independently of each other with true isolation, and Pop!_Shop will keep them both updated.

As we continue our Linux journey, we will encounter various applications which will require different forms of installation. We will address those as they are encountered.

At this point, I am ready to load all of my documents and personal data onto my encrypted disk so that I can start using the machine daily. If you have installed Linux Pop!_OS and made these configurations described here, you are ahead of the pack. You are more private and secure than 95% of all internet users by simply using Linux. You are ready to follow along with this new monthly column.

Every year, Linux gets better and feels more mainstream. Switching to Pop!_OS makes me no longer miss macOS. It seems just as nice, if not better. Pop!_OS feels fast, snappy, and well-designed. I know that I am making better choices about my computing activities by leaving the Apple and Microsoft ecosystems. However, this is only the beginning.

As we navigate Linux together each month through this series, I will explain how I rely solely on Linux every day. There will be many customizations, configurations, and installations as we go. I promise to offer many new applications which will make your daily computer usage more efficient and enjoyable. Eventually, you will forget all about Windows and macOS. For more information about System76's desktops and laptops, please visit <https://s76.co/System76Unredacted>. See you next month! ■

system76

THELIO DESKTOP COMPUTERS

Crafted with Intention in Denver, Colorado



WELCOME TO THELIO

The Thelio desktop line was born from the belief that humans are capable of anything. We believed that we could make an open hardware desktop that's powerful, compact, quiet, beautiful, upgradeable, backed by lifetime support, and manufactured in the United States—so we did. Powered by either AMD or Intel with a top of the line components, the Thelio is made to help you unleash your potential. What will you make with it?

LEARN MORE: [HTTPS://S76.CO/SYSTEM76THELIO](https://s76.co/system76thelio)



Image: Andrew Stickelman

HOW DID AMAZON'S CAMERAS ID ME?

By Wolfram Donat

By now I am sure you have heard that Amazon vans were recently equipped with an AI camera system. But what have you heard exactly? Vice magazine complained a bit about privacy, but mostly focused on a loss of income for drivers. Business Insider helped drivers vent regarding the nuisance of being on camera all day. CNBC tried to focus on the violation of privacy, but fell short of fully grasping the nightmare these cameras pose. In order to fully understand the system, I took it upon myself to test it, and maybe even fool it. In the end, I learned that everything Amazon told me about this system was not true. And every concern I had was justified.

While it's easy to say "Amazon is a private company and it can ask employees to be on camera all day"

I would agree. But there are tens of thousands of these vans on streets every day. The AI camera system is just one of many privacy issues. These are potentially mobile wardriving machines with the ability to identify and log everything about you, down to your face.

If you're an Amazon Delivery Associate, the process to start work is pretty straightforward. You log into "Flex", the Amazon delivery app. Then you snap a picture of yourself and the van VIN number (usually a VIN number converted to a QR code). This pairs you to the vehicle, allegedly. And the camera system is there to record traffic violations. But on a recent trip to take a van to a mechanic, the NetraDyne AI camera was able to correctly identify me without me pairing to the vehicle. We get alerts when mechanics take a van for a test drive and roll through

a stop sign. An "Unknown Driver" flag comes up with the alert and the violation. We always believed that that was because whoever was driving was not paired to the vehicle through the separate Amazon delivery app. While I'm sure the Amazon app can help them make the association, it really just meant that NetraDyne hadn't learned to identify that face...yet.

This was extraordinarily confusing. How did it associate my face to my name? At first, I contacted co-workers and asked them if they manually added my name to the system and to that violation. They didn't. Did the system itself know who I was just by being in the face of everything we were told. When the system was installed, the first thing Amazon told the contractors was that the system didn't keep or store the videos of your face; anyone concerned

with privacy could request the face to be blurred. As time went on, I never was given the option to blur my face. And it turns out that the face would be blurred only for contractors, and not Amazon itself. While not optimal, at the time I was happy to know that they didn't keep video recordings of my face.

But I never trusted Amazon. There were too many times they had given us contradictory information. So, in order to test this, the daily selfie I snapped for the Amazon delivery app was rarely ever my own picture. I mostly wanted to see how long it would take for the AI camera to realize the selfie picture didn't match who was in the driver's seat. I also didn't want a daily picture of myself on file with them. It turned out to be a good way to test if they actually relied on that picture at all. For the delivery app selfie, I used images of people of different races and genders. I never received any sort of alert or flag for an unknown or mismatched driver. It led me to believe that the selfie taken within the app was never really used for anything. You just needed to do it and it appeared as part of your profile on the app itself. It may be used for more than that, I just don't know. But the NetraDyne system can't possibly be using that to identify me. If it did, it would wonder why Salma Hayek is on file and the person in their driver seat looks portly and bearded.

Upon confronting the contractors I work with, no one had an answer. I started to believe that the system could've only identified me if it had always been recording my face, pairing it to my name/employee ID, and was learning from it. Furthermore, it needed to disregard the fake selfies I had taken. So the NetraDyne face videos were stored and associated with my name. And my morning selfie didn't matter at all. The camera system itself was able to ID me regardless.

As of last year, CNBC reported that Amazon's Prime delivery service has at least 30,000 vans. Unless you live in a very rural area, you likely see at least one a day. The tech that these vans are equipped with have the potential

to violate every aspect of your privacy. The problem comes down to consent. If three households in a neighborhood are active Amazon customers, does this give them permission to grab data daily from the remaining households? And what type of tech is onboard the vans? The most concerning aspects are specifically two pieces of tech. The ability and functions are never fully revealed by Amazon, even when asked over the course of years. Those two pieces of onboard tech are the aforementioned Amazon delivery app named "Flex" and the AI-powered camera system NetraDyne. When NetraDyne was installed, everyone needed to sign consent forms, but the system captures much more than just the driver.

Do you ever get an email with the photo of your package on your doorstep? That's courtesy of the Amazon Flex app. It grabs a current picture of the front of your house, and assesses that it's your house based on GPS...for your convenience, obviously. The first strange issue that I noticed with the Flex app is that even though it never used Wi-Fi, it was required to be on in order to use the app. The first excuse I was given for that was that it was used for GPS. Now, I know how GPS works, and yes, Wi-Fi does aid in accuracy, but our devices had offline maps for our regions. Even using those, the app itself wouldn't allow you to turn off Wi-Fi. As an amateur wardriver and Wigle enthusiast, my mind instantly realized that Amazon very well could be interested in scraping router names and IDs. At first I had no proof they were doing this. It wasn't until I installed a new router at home, received a delivery from Amazon, and was talking to the driver that I got my first inkling. The Flex app wouldn't allow him to complete the delivery. It asked him if he was sure this was the right place. And he needed to override the app to complete it. While not definitive, it helps the theory. It's entirely possible that the app has been collecting the data on my Wi-Fi access points and did not see that router this time and triggered the error.

Then one day, for no real reason, Wi-Fi no longer needed to be active

on the delivery app. It just didn't matter. I asked around, and not a single person—contractor or Amazon employee—could tell me why. But something else was required now to complete deliveries. Bluetooth. However, Amazon still has the potential to capture Wi-Fi. As the camera system has the NVIDIA JTX1 module at its core, and it has Wi-Fi. Maybe that explains this situation. Once the camera system was installed, we no longer required Wi-Fi to be active on the phones itself.

The NetraDyne camera system comes stock with four cameras. Two face sideways, one faces forward, and one faces the driver. According to the spec sheet, it captures 360 degrees of video. And even though Amazon claims it doesn't record anything other than traffic violations (for safety reasons), it has onboard storage to hold up to 100 hours of HD video. A recent update to NetraDyne seems to fly in the face of Amazon's claim. The FMCSA Crash Determination feature boasts of having an "always on" feature and is always recording, not just recording incidents. The system itself also has a Bluetooth antenna, usually mounted on the passenger side of the dashboard. The main reason for this is that it is supposed to record the amount of time spent out of the vehicle. When I asked how it actually knows what device I'm using, the answer was a bit strange. I was told that it's just "looking for devices", and it will be able to tell which one is the Flex phone. I think that was the most accidentally true response I've ever received. Of course, what they said was technically accurate. If I ran the Bluetooth scanner LightBlue all day while at work, I could definitely go through the list of devices I encountered and figure out which are mine. Since Amazon has a huge part of their retail business in Bluetooth and Wi-Fi connected devices, it's plausible that they are scanning your neighborhood to figure what's there.

Amazon has an HD camera system capturing 360 degrees of all activity in your neighborhood. It has the ability to detect faces and ID people and it could be scanning for Wi-Fi and Bluetooth

all of the time. For at least the driver's faces, Amazon was not honest (vocally) about recording, storing, or applying the video and data to AI.

What about OCR? The confidential tear sheet from NetraDyne boasts the ability to read street signs. It reads speed limit signs and will then check your travel speed. Couldn't Amazon also just put an off-the-shelf open source OCR on their back-end to look for other interesting data points? If I have a sign on my front lawn, will Amazon record that and associate it to my address? Who will that information go to? We don't know, and we can't rely on Amazon to be completely honest with us.

While they verbally told us no video of faces would be kept, they rushed everyone to sign a waiver for the NetraDyne system. Conveniently, the actual waiver would never actually open, but the page to agree to the terms worked just fine. I trusted that Amazon would not lie directly to its contractors. When we were told that

the faces wouldn't be kept, I believed them. I didn't care that the agreement for the cameras didn't load. I figured it was a very typical EULA or ToS-style monstrosity. I got it to download weeks later. It's a single page. It says the exact opposite of what we were told verbally. In their defense, they claim to "promptly delete" media after 30 days and claim they only store biometric strictly to confirm the identity of a person. But I wasn't signed into anything. They had no profile to compare it to. It saw a violation of speeding and decided to ID me, which shouldn't be possible if the system is operating how they claim it operates. In their own words, it should act like this: incident happens, camera system looks at your face, compares to your Amazon profile paired to the vehicle. In my case, the most crucial piece of info is missing. Except unlike the mechanic, they actually did retain my face and linked it to my name and ID all on their own.

The real kicker here is that even if you want nothing to do with Amazon, or even order from them under an

assumed ID and pick up at lockers, they're still in your neighborhood with surveillance tech. Your neighbors install their Ring doorbells and some of your neighbors invite them into the neighborhood to film you. Daily. If you didn't install a Ring doorbell and don't order from Amazon, too bad. They're going to be able to violate your privacy whether you sign an agreement or not. They may be telling the drivers that they will be careful with the info that they collect about drivers, but they say nothing, and don't answer to anyone, about how they use the trove of data they collect every day from the cameras alone. If I hop off of the MARTA downtown, and an Amazon van rolls by with cameras, I don't expect privacy. But that is much different than a van coming down your dead end or private road to serve a neighbor and being caught up in their digital surveillance. It's hard to know exactly what they are gathering, but at least we know what they are capable of collecting and can try to develop ideas to counteract their efforts. ■



INDUSTRY LEADING TECHNOLOGY AND A 24X7 SOC WORKING FOR YOU

Cyber threats are evolving rapidly. SMBs and Enterprise businesses are looking to their Managed Service Providers to provide them with cybersecurity solutions. Our managed SOC is highly-skilled in the constantly evolving threat landscape and will provide absolute security for you and your clients.



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

WHEN 2FA HARMS MORE THAN HELPS

By Michael Bazzell

Last week, I had a friend of a client reach out to see if I could help with a unique situation. Her phone had been stolen, and she could not access any of her accounts. I assumed this simply meant I would be purchasing a new device, setting up new cell access, and having a conversation about starting over. It was not that simple.

The issue was that this person had done most of the right things. She used a password manager, enabled two-factor authentication on everything, and even made sure that every credential she has was unique and randomly generated. However, this all required physical access to her device.

Her chosen password manager was cloud-based. While secure, she had no access outside of the app. If she wanted to log into her password manager from another device, she had to either verify a temporary 2FA code sent to her cell number or verify from the app. She had no access to the mobile password manager app, which was installed only on the device with her stored access credential for easy access. The phone was encrypted and locked, so there was a small amount of relief there.

The number on file with the password manager was her true cellular number, which she could not access. This number was associated with a prepaid account, and porting the number to a new SIM card could be problematic.

Worse, her phone was set to display notifications on the lock screen. If

she did request a temporary code, it would be received and displayed to the thief, potentially adding a new layer of exposure. Before I get to the solution for this, let's talk about ways to mitigate this scenario.

- Always have a backup of your password manager database. If you use a local manager, such as KeePassXC, this is easy. Simply duplicate the database file and store it securely. If you use a cloud-based option, such as Bitwarden, export your database regularly. Having a local copy allows you to access your credentials without the 2FA requirement.
- Never use 2FA with your true cellular number. That number is tied to your SIM card. Theft or loss of the device renders this layer practically useless.
- If a service allows a hardware device, such as a YubiKey, to be used for 2FA, choose that and consider a backup device as a secondary unit. Store the backup key securely at home.
- If hardware support is not available, consider a software token through apps such as Authy. While Authy receives a ton of criticism for their balance of convenience over complexity, the ability to synchronize your accounts across devices can save you from many headaches.
- Make sure you have backup access codes to any accounts which demand 2FA upon login.

Store these securely in your password manager in case you do not have access to your second factor.

- For accounts which only support a phone number for 2FA, create a VoIP number solely for this use. This could be a Google Voice number with strong hardware 2FA security, which is preferred due to their ability to accept short-code messaging.

The solution for her issue was complicated. We contacted the password manager to see what could be done. As expected, they could not help. Without the password and 2FA, they had no ability to access the account (which is a good thing).

We contacted the cellular provider to obtain a new SIM card attached to that account, but were told it would take up to 30 days. We could not wait that long. We finally went to a major cellular telephone kiosk and explained the situation, agreeing to purchase a phone with provided service. The sales representative was able to port the number from the previous prepaid carrier within an hour once my client provided all information from the account (name, number, billing address, and email). That was the scariest part for me. Any adversary could have done the same thing in her name. The final lesson here is to never rely on your true cellular number for anything. It is best if you do not even know what it is. ■



Image: Tony Stoddard

CHOOSING THE RIGHT WIRELESS PROVIDER

By Bobby Cyber

I enjoy experimenting with the privacy and security technology and techniques. One of my favorite things to experiment with is cellular services. The cellular services market is confusing and opaque. Even the words we use to describe these services (cellular, mobile, wireless, etc.) can be unclear. The market is also constantly changing. In my experience, experimentation is the only way to determine how well a wireless provider will work for you.

The primary focus of my research is price and privacy. Privacy seems to be the easy part. Choosing the most cost-effective plan for your needs can be difficult. I have used my research to help friends and family members save hundreds of dollars per year,

and I would like to do the same for you. My goal is to provide you with enough information to choose the right network, provider, and plan for you. Please note I specifically choose the word “right” rather than “best”, because your decision will likely include trade-offs between cost, coverage, and speed.

I suspect most readers to value privacy above all else. I also suspect many readers will have knowledge of and opinions about what constitutes anonymous or private cellular services, so I will not explain that in depth. Suffice it to say, most prepaid providers will allow users to create accounts and pay for services using “burner” email addresses, alias names, and any mailing addresses. Instead, I think it is

worthwhile to explain how the wireless market has changed since the wireless revolution began in the 1990s. Readers who never had a postpaid plan, or have already replaced their postpaid plan with a prepaid plan, can skip ahead to the “How To” guide on the next page. However, I think the history is interesting, and I provide examples of how expensive complacency can be.

Postpaid plans were the norm in the early days, but they excluded individuals with little or poor credit and those under the age of 18. A patent for prepaid mobile phones was filed in 1994. Early prepaid mobile phones were attractive to customers who were denied postpaid plans due to lack of credit, but were more expensive than postpaid plans.

That history stigmatized prepaid mobile phones, but that began to change in the early 2000s. A December 3, 2009 New York Times article by Jenna Wortham ([‘Frugal is the new chic’ in mobile plans](#)) said:

Any stigma attached to the phones - they are a common prop in any show or movie about gangs and spies - is falling away as prices drop and the quality of the phones rises. Prepaid carriers like MetroPCS, Virgin Mobile and Sprint's Boost Mobile division now offer sleeker models, better coverage and more options, from 10-cent-a-minute calling cards that customers refill as needed, to \$50-a-month, flat-rate plans for chatterboxes who want unlimited calling, web browsing and text messaging.

Nevertheless, many postpaid customers were unaware of the benefits of prepaid plans and stayed with their postpaid plans.

The market changed rapidly, and some customers stayed with discontinued postpaid plans, believing those plans would provide long-term benefits compared to the new plans that replaced them. Switching plans or providers seemed to mean forfeiting some advantage of being a long-term customer, and renewing contracts was an easy way to get new “free” phones from the carrier. At least one provider, Verizon, continued to charge postpaid customers the same monthly rate, but increased their monthly data allowance. This effectively provided postpaid customers with more data than they needed at the same price they were used to paying. If a customer did not know any better, they would continue to pay for more data than they needed rather than lowering their monthly cost.

One of the people I helped in 2020 was paying Verizon nearly \$95 per month for one smartphone with 8 GB of “shared” data, carryover data, and unlimited talk and text. This included \$70 per month for the “new Verizon Plan Large 8 GB”, and \$20 per month for one mobile device to access the “shared” data. On average, the

customer used less than 5 GB per month in a 12-month period, and only once used more than 6 GB, so the carryover data was useless. Today, that former Verizon customer is a satisfied Mint Mobile customer who has tried, usually unsuccessfully, to convince friends and family members to stop overpaying for mobile phone service. The Verizon network is better than the T-Mobile network used by Mint Mobile in the places this customer lives and works, but the T-Mobile network is good enough that the customer is not interested in paying more to access the Verizon network, even through a more cost-effective mobile virtual network operator (MVNO) like US Mobile.

Another person I helped in 2020 was paying Verizon nearly \$250 per month for four lines with unlimited talk, text, and data. This included \$110 per month for the “new Verizon Plan Unlimited” plan, \$80 per month for four mobile devices to access the shared data, and \$45 per month for Total Mobile Protection Multi-Device (TMP MD). The plan was “protecting” an iPhone 8 Plus, iPhone 7 Plus, iPhone 7, and an iPad. I will not opine on the wisdom of insuring those devices. Suffice it to say, the \$540 annual cost is currently more than enough to pay for a newer device like an iPhone 11 or iPhone SE (3rd generation). Today, that former Verizon customer is a satisfied US Mobile customer who pays less than \$50 per month for four smartphone lines sharing 6 GB of data on the Verizon network.

Step 1: Choose your networks

The most important aspect of finding the right wireless provider for you is identifying the network (or networks) that work in the places you need it most. There are three major networks in the U.S.: AT&T, T-Mobile, and Verizon. The only way to know for sure is to test all three in the places you need it most. This can be accomplished by acquiring a SIM card for each network or using an eSIM. I will not comment on the privacy implications of these choices. I encourage you to research your options and make the best choice based on your budget and threat model.

Step 2: Choose your services

Most plans include unlimited talk and text and a monthly data allowance. For example, Tello currently offers plans starting at \$10 per month for 1 GB, Boost Mobile currently offers plans starting at \$15 per month for 2 GB, and Red Pocket Mobile currently offers plans starting at \$20 per month for 3 GB.

First, carefully consider whether 5G access is important to you. T-Mobile has offered “mid-band” 5G since 2020 using spectrum on the 2.5 GHz band it acquired when it bought Sprint. AT&T and Verizon spent billions on “C-band” frequencies (between 3.7 GHz to 4.2 GHz) to expand 5G coverage in January 2022. I will not attempt to explain the differences between 4G, LTE, and 5G here other than to say I do not believe the reality matches the hype for most people. Not all providers and plans include 5G access, so read the fine print if this is important to you.

Second, consider whether you need to use your smartphone as a hotspot. This feature, also known as tethering, allows you to use your data on other phones or devices. Wireless providers use words like “hotspot” and “tethering” interchangeably, but not all plans include this feature. Some providers prohibit standalone hotspot devices but allow using smartphones as a hotspot. Hotspot data may be provided at slower speeds and lower limits than smartphone data, so read the fine print if this is important to you.

Step 3: Choose your providers

Until recently, I might have recommended using Red Pocket Mobile to test the networks, because they offer low-cost plans on all three major networks (GSMA = AT&T; CDMA = Verizon; and GSMT = T-Mobile).

SIM cards can be ordered online or purchased in-person with cash. I have tested with them in the past. However, recent customer service delays (hours, not minutes), have me avoiding Red Pocket Mobile. This may not be a problem if you activate the SIM cards, use them for testing, and abandon

them without the need for customer service. However, I encourage you to test with the provider you might use after testing, so I cannot currently recommend Red Pocket Mobile.

TracFone Wireless Inc., a subsidiary of Verizon, includes several brands (Straight Talk, TracFone Wireless, Simple Mobile, Total Wireless, SafeLink Wireless, Walmart Family Mobile, NET10 Wireless, Page Plus, and GoSmart Mobile). Straight Talk and TracFone Wireless offer low-cost plans on all three major networks. SIM cards can be ordered online or purchased in-person with cash. Both include 5G access, but Straight Talk provides more plans that include hotspot data.

Mint Mobile is a great way to test the T-Mobile network, but does not provide access to the AT&T or Verizon network. US Mobile offers low-cost plans on two of the major networks (Super LTE = Verizon; and GSM LTE = T-Mobile). SIM cards can be ordered online or purchased in-person with cash. All Mint Mobile and US Mobile plans include 5G access. My experiences with both apps, websites, and customer service have been good. In February 2022, US Mobile became one of the first virtual network operators to offer Two-Factor Authentication (2FA) to secure accounts. Mint Mobile does not currently offer 2FA.

All Mint Mobile plans include the hotspot feature at no extra charge. US Mobile custom plans also include the hotspot feature. These plans are great for testing purposes. However, the hotspot feature costs an additional \$5 per month with “Unlimited Bundles”, and \$10 per month with the “Unlimited All” plan, so I do not recommend these plans for testing. US Mobile shared data plans, available only on the “Super LTE” (Verizon network), also include 5G access and the mobile hotspot feature. This is a great option if you like the Verizon network and you need between two and ten lines after testing.

Last, but not least, AT&T PREPAID is also a good way to test the AT&T network if HD video and 5G access are not important to you. Only the

AT&T PREPAID Unlimited plan (\$50 per month plus taxes and fees with AutoPay) includes 5G access, and 5G mobile hotspot data is an additional \$10 per month, so consider other providers if this is important to you. Until recently, I might have recommended using FreedomPop to test the AT&T network, but Red Pocket Mobile bought FreedomPop in 2019. The FreedomPop app, website, and customer service are nearly identical to Red Pocket Mobile, so I suspect FreedomPop is suffering from the same customer service delays.

Step 4: Choose your plans

The amount of data you need depends on the amount of testing you need to do. For some users, places like home, school, and/or work may suffice. Frequent travelers may need more data and/or time.

Consider a total budget of \$100 to test all three networks. AT&T will likely be the most expensive network if you avoid Red Pocket Mobile and FreedomPop. The AT&T PREPAID 15 GB plan is currently the best value at \$40 per month. It includes 15 GB of “high-speed” (4G LTE) data, standard-definition streaming, mobile hotspot, unlimited talk & text to Mexico and Canada, roaming data in Mexico and Canada, and unlimited text to more than 230 countries.

For simplicity’s sake, consider using US Mobile to test both the T-Mobile and Verizon networks. The US Mobile Starter Kit includes both the GSM & Super LTE SIM cards for \$3.99, but there are several ways to get them for free, including using the promo code FREESIM. Choose the 18 GB for \$25 “bundled data” plan for each SIM card if you want to stay within the \$100 budget.

Step 5: Prepare to test

While you are waiting for your SIM cards to arrive, consider what mobile device or devices you will use to test. Again, consider your options and make the best choice based on your budget and threat model. It might be ideal to simultaneously test all three networks

using three new 5G devices. However, this is likely financially unfeasible and practically difficult without specialized equipment. If you have no immediate plans to replace your mobile device, consider using the one you already have. Otherwise, time testing to coincide with replacement.

In addition to hardware, consider what software you need to test on your mobile device. At a minimum, prepare to test firewall and VPN apps. Anything you use to protect your privacy and security from the network may reduce speed. This could include internet browser apps and configurations. Be prepared to test the VoIP and secure messaging apps you rely on too.

Choose a speed test app to use for your testing, and plan for recording your test results. Consider both the privacy implications of your choice and the data it will provide. Do not rely on the app to keep records for you. Prepare to take your own notes, including the date, time, and location of each test. Consider using a spreadsheet.

Plan your testing times and locations based on your needs, but plan to allow for plenty of time for each test. Plan multiple tests with each SIM card, and allow for time to restart the mobile device between SIM cards. It may take a little time to connect to each network. Consider testing in a location where you have internet access on a computer or another device, so you can contact support if you have any problems during your tests. Make contingency plans. Planning will help you make the most of your testing time and help prevent the need to pay for another month.

Step 6: Test your networks

Once you receive your SIM cards, activate them and execute your testing plan. If you are fortunate, one network will be the clear winner. If not, you may consider a dual SIM device that allows you to switch between two different mobile networks, but that is project for another day. ■

THE OSINT CORNER⁷

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 benefits of working with and instructing a wide variety of teams, is the opportunity to identify common mistakes and pitfalls which we tend to run into during our open source intelligence work. The following are some considerations and potential issues that I see arise often, both with new and experienced practitioners.

Issue: Rushing into the research phase without taking the time to organize your investigation and environment.

Considerations: We always want to stop and take moment to identify the key questions that need answering and our overall mission goals. We should also make sure our workstation, accounts, and tools are all sufficient for the task at hand. Are we preventing cross contamination with other investigations? Are we protecting our connection and workstation at a level appropriate for the operational security needs of our mission? Is this a long term case that may warrant creating a new virtual machine and new investigative accounts? These are all good questions to ask ourselves before diving in.

Issue: Failure to capture key findings prior to them changing or disappearing.

Considerations: When you find that pivotal Twitter post or that incriminating image on a blog, we should consider preserving it immediately so that we do not lose it if the target or the platform deletes or modifies the content. There is nothing worse than finding a case-breaking lead or piece of evidence, only

to go back an hour later and find that it is no longer there. Sure, you can hope to recover it using something like Google cache, but that is an unnecessary roll of the dice. Best practice is to at least take a screenshot of any key intelligence as you discover it. Even better is saving it in a forensically sound manner to preserve a page or post at the code level.

Issue: Using third-party tools or services which provide data, but for which you may have no understanding of where the data came from.

Considerations: The impact of this scenario will depend on your mission and final disposition of your case work. If you are like me and much of your work ends in a court case, you will need to be able to explain to a jury or other third party how the intelligence was recovered, and why we are confident that it is accurate. We need to properly source or provide attribution for our findings. Using free or paid tools which "spit out" lists of data is not valuable unless you know where that data came from. This is even true with our own custom OSINT toolset, and why we always encourage users to get under the hood and learn how those tools work.

Issue: Failure to understand and abide by applicable policies and laws.

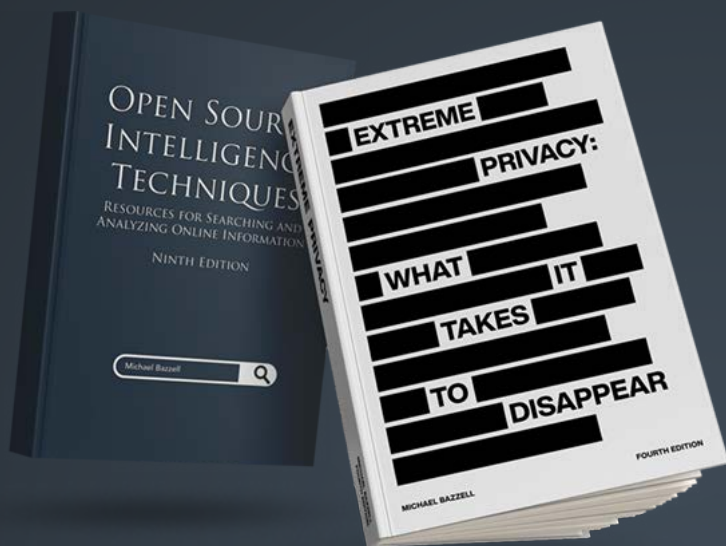
Considerations: We need to understand not only the local, state, and federal laws where we work, but also be aware of additional policies and

restrictions imposed by our employers. One area that is often overlooked when doing contract work is taking the time to clarify with clients any restrictions due to their own policies and legal constraints. If you are acting as their agent, you likely are beholden to additional restrictions and limitations. We never want our actions to damage the reputations or legal standing of ourselves, our employers, or our clients. If there is any murkiness, consider further research into applicable laws/policies or if available consult with legal counsel.

Issue: Wanting credit where credit is not appropriate.

Considerations: One of the many odd things about working in the intelligence field is that if we are doing our job correctly, we should be drawing very little attention to ourselves. This is counterintuitive to the current culture of broadcasting successes on Twitter and elsewhere. Almost all of the work we do in truth belongs to others: clients, victims, employers etc., and it is not our place to spike the football for internet points. This is ironically one of the tricky things about instructing tradecraft. Most of my best examples of OSINT work, I can never share with students. This will also ring true to those of you in the intelligence community, because, in a world of "show us stats to prove your worth", we are a sub-sector that really should be quiet most of the time and focused on getting out ahead of infrequent, but high impact, critical incidents. ■

New 2022 Privacy & OSINT Books



- ✓ Hardcover & Paperback
- ✓ New & Updated Content
- ✓ 500+ Pages Each @ 8.5 x 11
- ✓ Our Full Playbooks
- ✓ Supports This Free Magazine

Order at IntelTechniques.com

OSINT & Privacy Video Training

90+ Hours of Video Training | Optional OSIP Certification

Register at IntelTechniques.net





Image: Sunil Ray

EULOGY FOR THE IPOD TOUCH

By Michael Bazzell

Last month, we lost the iPod Touch. Many readers will be surprised at my sadness over this news, but hardcore privacy enthusiasts will understand my pain. The iPod Touch played a strong role during my privacy adventure.

When I relied on an iPhone as my daily mobile communications device, I refused to allow it near my home. Apple's iOS constantly collects data about usage, including location, and sends any details back to Apple's servers. Since the device possessed an active cellular connection, there was always a risk of exposing my home address. Since iOS resets cellular, Wi-Fi, and Bluetooth connections after an update, airplane mode was never enough for me.

That is where the iPod Touch came in. It was a low-powered, fully-functioning, iOS device, but without the cellular connection. I could install all of my desired communications apps, each

connecting only through home Wi-Fi (protected by VPN), and I never worried about my location being exposed. This also served well for many of my clients under extreme threats.

I stopped using an iPhone and iPod Touch in 2020. I could no longer accept the constant telemetry being collected by Apple, even if they did not know my true location. I switched full-time to a GrapheneOS device and never looked back. The iPod Touch was retired to the closet of old devices, and I maintained a separate Pixel 4a in my home for access only via Wi-Fi.

Many people have asked me if the two-device lifestyle is still important for those who have adopted the GrapheneOS mobile device. For rare cases, I do believe there is a benefit to two devices. However, for most people, I believe it is overkill. If you possess a GrapheneOS mobile device and the discipline to use it properly, I think having that device in your home is fine. There are two rules which must

be followed at all times if you take your privacy seriously.

1. The device should be placed into airplane mode before you arrive home. This prevents your cellular provider from documenting the location of the device overnight, confirming where you sleep.
2. You must disable Wi-Fi and Bluetooth when you leave your home. This prevents any wireless beacons from collecting your device details, and any malicious devices which could track your movements.

Some people have asked me if I would be stocking up on iPod Touch devices before they completely disappear. I will not. They served me well, but I have no more need for them in my life. As of this writing, Apple is completely out of stock, and prices on used devices seem inflated. Life goes on. ■

THE HOME ADDRESS DILEMMA AND FORM I-9

By Rob Hoffmann

My father often said, “Don’t lie about anything you can’t talk your way out of.” This is good advice, especially useful if you get audited by the IRS for a dodgy tax deduction. If your attempt to justify it seems plausible, they might make you pay the extra tax, and possibly a late fee, but you probably won’t be accused of actually trying to defraud the government. But an out-and-out lie might get you into trouble.

I’d like to think the same applies regarding the home address issue, which is perhaps the biggest concern among privacy enthusiasts.

“How can I keep my physical address private and not lie on government forms? What can I get away with?”

The answer is: it’s tricky. The official answer is to never lie on a government form that you sign. Sometimes you might be able to get away with it if the address line says simply “Address”, or “Street Address”, because then you can use a P.O. Box (no one would accuse you of pretending you actually live inside a P.O. Box!), or, in the second case, the “street address version” of your P.O. Box, which a lot of U.S. Post Offices will assign you (if you rent a box) in order to receive packages from merchants or shipping companies (like FedEx) which will not ship to a P.O. Box. If a form doesn’t specify what kind of address (or street address) it wants, you can very likely talk your way out of being caught for not putting your residential address.

Unfortunately, the Patriot Act, which became law after 9/11, which intended to help thwart criminal and terrorist activity, has made true privacy for law-abiding citizens nearly impossible for all but the ultra-wealthy (who can find a way around most any rule, it seems), and people who are able to have official

nomad status. Many government forms now specifically ask for a “physical” or “residential” address, and make it very clear that P.O. Boxes and CMRAs (commercial mail receiving agencies) are not acceptable.

The biggest obstacle for many, with respect to keeping one’s physical address private, has been the dreaded Form I-9, which is the document you must fill out if you are to work for a company as an employee. This document is how you attest citizenship or legal residential status in the U.S., and thus the ability to legally work as an employee. This form asks for a physical address. The instructions to the now-outdated form say, “Do not provide a post office box address (P.O. Box)”.

Instructions for Form I-9 now say, “If your residence does not have a physical address, enter a description of the location of your residence, such as “3 miles southwest of Anytown post office near water tower.” So even living “in a van down by the river” (the address of motivational speaker Matt Foley, the beloved Chris Farley SNL character), is still acceptable. They really want you to put down your residential address.

This is a deal-breaker, and it is why being self-employed (or working for “fee” income instead of “salary” income), is the choice for many privacy enthusiasts. Unfortunately, many people who need to earn income (and that is most people) cannot choose how their payment is structured.

One important thing to note about I-9 forms, according to the U.S. Citizenship and Immigration Services:

Form I-9 should be kept on file for 3 years after the employee’s start date or 1 year after the termination date of that employee, whichever is longer, and you’ll make this calculation at the time your employee leaves your employment.

Remember: employers do not send completed I-9 forms to the government. They keep them on file, and they only show them to the government if requested to do so (which is rare). If the paper forms are locked in a drawer somewhere, it’s likely that no one will ever see the address on the form. In any case, this doesn’t seem to be a reason for worry anymore. Here’s why:

https://www.uscis.gov/sites/default/files/document/questions-and-answers/FormI.9.Questions_and_Answers111716.pdf

The above document from the U.S. Citizenship and Immigration Services, which is in Q&A form, states:

[...] employees can enter their current residential or P.O. Box address [...] Preparers, translators and employers may not enter P.O. Boxes on Form I-9.

The new I-9 form, though it still asks for a physical address, no longer contains the “no P.O. Box” language.

Reportedly, the instructions changed to protect people in confidentiality program (e.g. victims of stalking). It’s clear that the government does not encourage non-residential addresses on the form, but it looks like they won’t bug you if you write your P.O. Box on the form. (Do *not*, however, use the “street address” version of that P.O. Box, because the USPS, as a condition of letting you use that address, states that you are not allowed to claim that it is your “residential address”).

<https://www.lawlogix.com/glitches-and-guidance-relating-to-the-new-form-i-9/>

This is great news for employed people. I recently started a new temporary job, and I put my P.O. Box in the address field of the I-9, and no one objected. Score +1 for privacy. ■



FUN WITH RADIO RECEIVERS

By Michael Bazzell

I have a thing for terrestrial radio signals. It started when I was a child. I was given a portable AM/FM radio which I carried with me while I walked to school every day. I would listen to a man read the local news from my small town, and occasionally I would hear a name I knew. It seemed magical. Some stranger across town was talking into a microphone, and my battery-powered box was intercepting the signal, then creating an audio wave which I could hear. Today, that sounds ridiculous. Back then, it was my internet. This was a time before personal computers, cell phones, and any way to contact others when not near a landline telephone.

My grandfather had explained to me how a radio wave works, so I had a very minimal understanding of the process. That radio was always by my side and I had memorized all of my local stations. I knew that 1120 AM was KMOX and they had a call-in trivia show every Saturday night. 550 AM was KTRS and they had a show about pets on Sundays. Of course, 94.7 FM was KSHE "95", which

made no sense to me. I knew my way around the dial. One night, I started searching for anything new which I had not heard. Around 880 AM, I heard a voice new to me. He was talking about cities I had never heard of. After some time, I realized I was listening to a local radio show in Nebraska, several states away. How was this possible?

I didn't know it at the time, but I was DXing. DXing is the search for distant radio signals. Listening to faraway radio on the AM band is only one small piece of this hobby. In North America, most AM radio stations fall between 530 kHz and 1710 kHz. Any functioning AM radio should be able to pick up local stations, but why did I hear Nebraska at Midnight?

Let's discuss the ways in which AM signals go from a radio station's tower to your radio. Once the AM radio signal leaves their antenna, there are two components which make up that signal. Groundwave signals travel along the ground while skywave signal travel up toward the atmosphere. The terrain dictates how far a groundwave signal can travel, while atmospheric

conditions determine the length of skywave transmissions. Sunlight is a big factor in the ability to receive these transmissions.

During daylight hours, you typically can only hear AM radio stations close to you. This is because you can mostly hear the groundwave signals traveling through the terrain because the sun is creating a "D-layer" which energizes the atmosphere. This layer absorbs skywave signals, preventing them from traveling a long distance. Therefore, if the groundwave cannot reach you, you hear nothing.

When the sun sets, this layer breaks down. Skywave radio signals can now bounce around the atmosphere, bumping into earth (and our radios). This is why a Nebraska radio station was crystal clear in my St. Louis basement at Midnight. When the sun rises, the atmosphere changes and we are stuck with local AM stations again. This is why listening to medium wave (530-1710 kHz), short wave (3,000-30,000 kHz), and long wave (1-300 kHz) signals is always best at night.

How far can the signal go? Well, that depends. I have been on an island in the Caribbean listening to broadcasts from South America, Africa, and Europe. I have been on the west coast listening to shows from China, Japan, and Cuba. I once camped in the Midwest and listened to a pirate radio station talking about telephone hacking techniques. I know, I was a nerdy kid.

There is also the issue of wattage changes at night. Many stations are forced by the FCC to reduce their power or cease operating at night, in order to avoid interference to other AM stations. This allows other larger stations blasting at 50,000 kilowatts to break through over longer distances. As an example, none of my local stations offer the show Coast to Coast AM. However, once my local stations power down, KFI 640 from Los Angeles can be heard clearly. They offer Coast to Coast nightly at 10 PM Pacific time.

I suspect you are wondering how any of this is related to privacy, security, or OSINT. Let's reel this in. Radio signals are one of the last anonymous ways to ingest information. They do not require a computer, internet access, IP address, web traffic, cached files, website cookies, or login credentials. They do not log your listening history or collect analytics about the shows you like. There is no evidence of your activity. This is a rarity today. Furthermore, radio can be a great source of OSINT. I have recently listened to signals from Russia and Ukraine, and BBC broadcasts being sent to those locations, through long wave at 198 kHz. That information is much more interesting than what my local morning show anchors think about things.

At this point, I will assume you are either interested in radio frequency monitoring, or you would have moved on to the next article. Let's talk about specifics. The first consideration is hardware. What radio works best? If you are serious about long-range listening, you will need a radio which monitors the entire 1 kHz to 30,000 kHz spectrum. These are commonly called short wave radios, which is a bit misleading.

You will also need a radio which supports an external antenna. While you could use the embedded loop antenna included with most units, you will be severely limited with your listening options.

I currently rely on a Sangean ATS-909X2 (<https://amzn.to/3MYRwVC>) or a Tecsun PL880 (<https://amzn.to/397WoZW>). I like the Sangean better, but those are getting hard to find. Both have the desired range and external antenna capability. A portable wire antenna (<https://amzn.to/3KYWr7J>) will bring in much more than the embedded loop, but not as much as a true outdoor antenna. I have my Sangean connected to an outdoor sloper antenna, which I made from a few hundred feet of wire and a 20' pole. Maybe we can discuss that in a future article. After sunset, I can listen to radio broadcasts from dozens of countries in multiple languages.

That brings us to short wave signals. If you possess a standard AM radio, you have reached the limits of your DXing. If you have a short wave radio, there are endless opportunities. Many short wave radios emphasize the use of "bands", which are defined ranges of frequencies which can be more active than others. Each band is associated with a number followed by "meters", and the higher the number, the lower the frequency. The following are the bands with their designated ranges.

120 meters	2300-2495 kHz
90 meters	3200-3400 kHz
75 meters	3900-4000 kHz
60 meters	4750-4995 kHz
49 meters	5900-6200 kHz
41 meters	7200-7450 kHz
31 meters	9400-9900 kHz
25 meters	11600-12100 kHz
22 meters	13570-13870 kHz
19 meters	15100-15800 kHz
16 meters	17480-17900 kHz
15 meters	18900-19020 kHz
13 meters	21450-21850 kHz
11 meters	25670-26100 kHz

To me, these ranges don't mean much. Plenty of the frequencies which broadcast content interesting to me fall outside of these ranges. Therefore, if your short wave radio pushes you to

scan only these bands, push back. One example of this is a nightly broadcast on 5085 kHz. It is an "oldies" style of music program available every night, broadcasting from Tennessee through 100 kilowatts of power. I often use this frequency as a test to see if my antenna is optimally placed. I have received this broadcast as far west as Nevada. As you may have noticed, it is outside of the common bands.

Some may wonder how they will ever find anything interesting to listen to with so many possible frequencies. That is part of the fun. I find the rotary tuning dial on the Sangean makes it easy to scroll through ranges of frequencies quickly and efficiently. I also prefer a radio which allows direct entry of a frequency, as I have many of my favorites memorized.

What will you hear? A little bit of everything. The most common short wave frequencies will broadcast an assortment of music, news, religion, foreign language, and the occasional interesting amateur screaming about the end of the world.

For OSINT purposes, I am mostly interested in international news broadcasts, especially those from countries which do not have a voice in my American papers. I also like to listen to the area around 27,000 kHz to hear my neighbor on his CB radio telling the world about his problems.

This initial article for this series is only the beginning, and sets the pace for future issues. We have barely scratched the surface. My plan is to present a monthly article discussing a unique area of radio listening. Pending topics include short wave stations, long wave broadcasts and beacons, pirate stations, citizen bands, computer-controlled SDR's, hardware reviews, and even remote-controlled radios monitoring from other countries. There is a lot to this hobby. The bands are still very active.

I am always open to guest articles on this topic. Are you a Ham or DXer? Tell us your story. ■



Image: Ludovic Migneault

READER Q&A

By **UNREDACTED** Staff

Do you have a question or need clarification about a privacy-related topic? Submit it to us for publication consideration at [UNREDACTEDmagazine.com](https://unredactedmagazine.com). If you have questions, other people are wondering the same thing! Please make sure your submissions are actual questions, and not vague statements with a “?” at the end. Here are questions from last month.

Q: How do we know our emails to you are secure? What are you doing to protect contributors?

A: You don't. Any email you ever send to anyone could be abused. However, we do take your contributions and privacy seriously. We host our email with ProtonMail, which is encrypted at rest. No one but our staff can access your emails from within that account. If you send email to us from your own ProtonMail account, then the entire conversation is encrypted within their network and safe from external eyes. After every issue is released, we permanently delete all email sent to our staff email address. This way, we can not be compelled to hand over any communication in the event a U.S. court order was received. You can read more about our privacy policy on our

website. Email is broken, though. Never use it for anything vitally sensitive.

Q: The Firefox browser gives the option (under Settings > Network Settings) of sending the domain name to the DNS server using an encrypted HTTPS connection (instead of a plain text one). Is this a suggested setting? Should it be done on a firewall instead? According to the link above, Firefox uses the services from a third party (i.e. Cloudflare). It seems these third parties need a way to profit from providing that service. Is this another case where the user's information is the product?

A: If you have a firewall with encrypted DNS, this might be overkill, but no harm in doing both. This only

covers browser queries, and nothing from your OS, which is why a firewall is better. Cloudflare makes their money in other ways, and their DNS has been audited by a third party. I currently prefer NextDNS for DNS and filtering.

Q: My business would like me to start traveling again. How should I get around at my location? Should I rent a car or use Uber/Lyft? I have been trying to figure out how to rent a car privately, but most places require a photo ID. I have thought about using Uber, but I'd rather not download it, since it will basically track my phone. Please let me know what you recommend.

A: Rental cars will always (and should) demand your driver's license. There is no such thing as anonymous car rental.

However, what are you trying to hide? If your home address is not on your DL, does letting the car company know your true identity fit within your scope? If you want to be more anonymous, Uber/Lyft are preferred. Aged accounts under an alias tend to work fine. Creating a new account will be more strict about verification. Both record your travel forever. I keep a secondary Android profile with Lyft in an alias name installed. I switch to it when I need to use the service and reboot the phone to the first profile after I am done. This is not 100% anonymous, but they do not know my true name. Payment is through Privacy.com. I never use it near my home.

Q: I can't plant my flags at all, because I'm not sure if it's really a good idea to read my SSN over the phone (when I'm the one initiating the call). Can you confirm for me, is it safe for me to read my SSN over the phone to plant my flag?

A: If you are calling a bank or other institution which already has your SSN, I see little harm. I would rather say it over the phone than email it or enter it online. Most of our SSN's can be purchased for a few bucks, so I don't see them as secret data today.

Q: I'm going to perform a "digital reboot" per the Extreme Privacy book. Would my real name be any more private if I used one computer (Linux) when using my real name and used a second computer (Linux) only when using an alias? (i.e., Can devices be linked with names shown or entered on websites?)

A: For most people, that is overkill. I would rather see you practice good OPSEC on one machine. If you are conducting covert government missions, then yes, you should isolate your identities. If you are ordering Amazon in an alias while checking your true email, you can get by on one machine with better habits, such as a dedicated browser for personal, and other for alias, and a reliable VPN. If that seems reckless, you could dual-boot Linux with a secondary alias OS, or use a VM. Many clients keep a VM

ready with an application-based VPN within it set to connect to a different server than their home VPN. They use that for anything they do not want to associate with their real name. Two separate physical computers on the same network would do little good.

Q: When using tethering, should we enable VPN apps both on phone and laptop?

A: It depends. If you are tethering to a Mac and don't want Apple to know your true IP before your laptop VPN kicks in, then yes. If you simply want to protect your web traffic from knowing your true IP, I would run the VPN on the laptop for better speed.

Q: What will you do if VeraCrypt has some issue? Any redundant options?

A: I guess that depends on the "issue". If they were found to be doing nefarious things, I would rely more heavily on my full-disk encryption to protect my data. You can use LUKS encryption of an external disk within Linux if needed.

Q: I am very frustrated. I have several VoIP numbers through Twilio, but have constant issues making them all work the way I want them to. Do you have these issues?

A: Absolutely. If you listen to my podcast, you have heard me complain about self-hosted VoIP, while other times I praise the ability to eliminate middle-man services. Only those with adventure and patience should try to go the DIY route. If you need stability, or hate fussing with ever-changing technologies, just go with MySudo. I use MySudo numbers for calls more than anything else because they just work.

Q: MB, you always recommend using Firefox Focus on Android. To me, Firefox Nightly seems to make a lot more sense. With Nightly you have access to about:config where you can fully harden it the same way as a desktop browser. Additionally, you can install add-ons like uBlock Origin and Privacy Badger. It also has tabs,

which is a key feature that is missing from Focus. So why do you prefer Focus over Nightly?

A: All fair points. Overall, I like FF Focus because it is extremely minimalistic and wipes out all browsing history by simply closing the app. Also, I use NextDNS for content filtering which eliminates most of the need for uBlock Origin. That all being said, I have Firefox, Firefox Focus, Firefox Beta, and Firefox Nightly all on my mobile device. FF Focus is used for all quick website visits or search queries. It is my default browser. It gets wiped out on its own when the app closes or I go "back" into an app which opened a link. I like that. It takes 95% of my web usage. The other "full" versions of FF are each used for a specific purpose, such as keeping me logged into a specific service or site. I can then create a home shortcut to that version of FF, set the necessary service as the home page, and treat it as a single-use browser which stays logged in. Since I use FF Focus for all browsing, the full FF apps do not get hit with third-party cookies or cache. They stay isolated. Each person is unique, and their mobile browser needs are equally as unique. Always do what works best for you.

Q: Regarding the article in issue 001 on maintenance videos, this was written: "This displayed over 1,000 videos beginning with my relative's unique entry, including '<LastModified>2022-04-25T15:27:55.000Z'. I now know that this vehicle inspection occurred on April 25 at 3:27 pm (in an unknown time zone)", Mr. Bazzell stated "unknown time zone" yet it is clearly marked Zulu (Z). Am I missing something?

A: Zulu is a military name for UTC or GMT, which is a global time at the Zero Meridian. Knowing the date and time presented in this format does not tell you the local time zone from where the video was uploaded. Therefore, you would not know the location (or the local time zone).

Q: I own a small business that I run out of my house in Missouri. For my business name I must file a "Registration of Fictitious Name" form. The state does not allow P.O. Boxes in this form—physical address only (I have tried—they manually review all submissions). The address provided will appear in a publicly searchable database/website. Any advice on how to keep my home address off this publicly searchable website?

A: I can't speak to your specific situation or Missouri law, and I am not providing legal advice, but I can share an anecdote. I once had to provide an official physical (non-CMRA) address which would become public record. I booked a hotel room for one night and completed an online registration form while there which required a "Current physical address". I provided the hotel address and even the room number as to be completely transparent. I then booked a second stay 30 days later and told them I may be receiving a package. When I arrived a month later, they were

holding the letter for me, and the hotel address was published online without scrutiny. Long-stay hotels seem to work best.

Q: For the person new to digital security and only familiar with Windows-based platforms, can you recommend a free or affordable site or course to learn more about DIY personal digital security, Linux etc.? Something that goes beyond following the commands in your Extreme Privacy book?

A: I would revisit the book (Extreme Privacy), as it is much more than "commands". It is over 500 pages of content to help with the very thing you are asking. The first four chapters (1/4 of the book) are dedicated to the tech side of things. If that doesn't scratch the itch, I would create some Linux VM's and work through any issues. The internet can solve any problem you find.

Q: What is telemetry? (Yes, I googled it and have trouble making

sense of the results) How is it different from an analytics service like Google Analytics?

A: That is a great question, especially since the term is mentioned here often. My definition would be the persistent collection and transmission of usage metrics and other data associated with a specific digital product or service to a third-party server. In other words, the constant analysis of your information while you use a product, such as MacOS or Windows. In one example, Apple collects data about every application you launch from your mobile device or computer, then analyzes your usage for their own benefit. Is Google Analytics telemetry? I guess it is in a way, but I make an important distinction. It goes back to the word "persistent". Your Apple or Microsoft operating system is *constantly* collecting data. Google Analytics can only collect data when a website hosting the code is visited (unless you use uBlock Origin to prevent this). However, there are similarities which are open to interpretation. ■



**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

OSINT BOOK: UBUNTU UPDATES

By Michael Bazzell

If you have my OSINT book (Open Source Intelligence Techniques, 9th Edition), and you are creating your first OSINT virtual machine, you may have noticed some new issues. The book was written using Ubuntu 20.04 as the Linux operating system, and Ubuntu 22.04 has since been released in April. While the new version of Ubuntu looks very similar to the previous LTS option, there is one huge difference. Firefox is now included as a Snap package. The look and feel of Firefox is the same, but many things changed behind the scenes.

First, the steps in the book to download and apply a Firefox profile with customized add-ons, bookmarklets, and settings do not work as printed in the book, because the path to the Firefox app has changed. Profiles must now be copied to the following folder.

```
| /snap/firefox/common/.mozilla/firefox/*.default
```

Next, the Firefox icon might be missing from your build because of this same path change. Instead of adding a shortcut for "firefox.desktop", you must now specify "firefox_firefox.desktop".

Finally, the search tools shortcut was broken by the 22.04 upgrade because the Firefox Snap package now requires the path of a local file to be included within single quotation marks. The 'tools.desktop' shortcut file now includes the following line.

```
| Exec=firefox '/home/osint/Desktop/tools/index.html'
```

These are all minor changes, and many people will never notice if they simply follow the online steps. I modified the following details within the book login portal on May 5th, 2022:

- Updated the "linux.txt" Linux Steps file to reflect path changes for Firefox in Ubuntu 22.04.
- Updated the "linux.sh" automated installation script to reflect path changes for Firefox in Ubuntu 22.04.
- Updated the "linux.txt" Linux Steps VM Configuration instructions due to a new slight change with VirtualBox and Guest Additions.

If you use the URL and credentials from your book, you will see these changes. As long as you are following the updated online TXT files during your build process, all should function normally. This is why it is always vital to check for updates on the site while following the book. ■



This magazine serves as a compliment to the weekly podcast, which can be found at [IntelTechniques.com](https://www.inteltechniques.com). Below are summaries of the episodes from last month.

260-Google's New Policy Change

Discusses Google's new data removal policy, the first issue of UNREDACTED Magazine, and numerous privacy & OSINT updates.

261-A Client Stops By

A client stops by to discuss his recent full privacy reboot, plus the latest news.

262-Brief Updates

Provides brief updates to the show, magazine, and latest privacy news.

263-Proton Changes & New Breach Lessons

Discusses the latest Proton changes and some new breach data privacy concerns (and investigation benefits).

LETTERS FROM READERS

By Michael Bazzell & UNREDACTED Staff

Do you have something to get off your chest or a quick tip which may benefit readers? Submit it to us for publication consideration at [UNREDACTEDmagazine.com](https://unredactedmagazine.com). Here are selected correspondence excerpts from last month.

"Dash Cam Stories" by Anonymous:

I have another reason to own a dash cam. I live in a county which allows drivers to sign a complaint against drivers who have allegedly committed a traffic violation. An officer does not need to witness anything, and the fines are steep. Last week, I accidentally pulled out in front of a speeding driver. They got mad and rode my tail. I refused to speed up and they could not pass. They called the Sheriff and said I was driving aggressively and "road raging". The deputy pulled me over and allowed the other driver to sign a complaint against me. Before the paperwork was finished, I convinced the deputy to look at my dash cam of the incident. He watched as I drove normally, and then refused to allow the complaint. He asked if I wanted to sign a complaint against the other party for filing a false police report, but I declined. Going to court is not very privacy-friendly.

"Twilio Updates" by John:

I just went through and set up my Twilio numbers and the code is almost right, but needs one change. With the incoming calls bin, the sip URL address is wrong. You are not allowed to specify a local server in the address. For example, "6666666666@6666666666.sip.us1.twilio.com" should be: "6666666666@6666666666.sip.twilio.com". With the previous one it goes straight to voicemail (if that's set up). It seems the local server is

decided when you set up the Linphone application, as in that URL you specify "us1" or "us2" or whatever.

Editor's Note: We tested this with the original text and calls came through fine (without forcing to VM). We tested this alternate option and it also worked fine. We are not changing the tutorial since it works as described and is the official Twilio guidance, but we will present your modification here in case others have issues. You may have something else unique going on.

"RFID Bag Review" by Jun:

Those who travel frequently are no stranger to the sales pitch of Radio Frequency Identification (RFID) blocking. Many RFID-blocking products are available and are famous in wallets and passport holders. On the other hand, backpacks have never maintained their integrity, especially for Everyday Carry (EDC) enthusiasts. Target has a simple-looking sling bag that took me a few months to pull the trigger to ultimately purchase: "AntiTheft RFID Sling Backpack Gray". The RFID sales point on any sling bag has never met anyone's expectations from my experience. To my surprise, its other features have made this specific sling bag my primary everyday bag.

As predicted, RFID-blocking is terrible, so don't count on it. However, this sling bag has become the mainstay of my EDC gear. A Plain Jane style is

fantastic since it makes you less visible in public, and there is no prominent branding. Bring forth the Jason Bourne in you. Initially, I didn't notice this ingenious design. The zippers can clip to a ring at the end to avoid accidentally opening the bag. The lock mechanism is a minor feature that momentarily becomes a deterrent for those looking for easy prey in densely populated regions. The "anti-slashing" fabric outperforms expectations. I wouldn't rely on it as a defensive weapon, but the material is sturdy enough that I've let my dog play with it, and it has survived. So if you're a tourist in an area known for thieves slicing open bags as you walk, this would be a significant bag to avoid such troubles.

Overall, it was worth the purchase, significantly since I use it every day. The sling bag is small enough to leave my keys, three SLNT wallets, my GrapheneOS device, wired earbuds, and flashlight at all times. I can leave this next to my front door when I'm home, then grab and go whenever I need to run errands. If I know I'm out the entire day, it's big enough to fit more stuff like a portable charger, USB cables, and a portable gaming console. Let's say you want a minimalist and defensively practical bag. In that case, I believe this is an excellent first EDC sling bag for a gray man's lifestyle.

"OSINT Bookmarklet Update" by Anonymous:

I thought I'd share a bookmarklet that I use daily, though not OSINT related, but rather if you want to use Google to search for a string on the site you're on, click this, and it essentially performs a "site:thesiteyouareon.com <string>" search on Google. I've found it very useful, provided you want to perform that kind of query, which, for me, happens almost daily, if not hourly. I call it "search.site". The JavaScript code to paste in the URL for the bookmarklet is:

```
javascript:Qr=prompt(
'Search%20Site%20
for', '');if(Qr)location.
href='http://www.google.com/
search?&q=site:'+encodeURIComponent(
window.location.
hostname)+'+'+escape(Qr)
```

Editor's Note: This works well. In Firefox, I chose the option to "Add" a bookmark, copied and pasted the code, and saved it to my Bookmarks Toolbar as "SITE". When I am on a target page and click this button, I can enter any

keyword and Google executes a site search as intended. I think this could be very useful to OSINTers.

"Skype OSINT" by Mishaal Khan:

When someone adds you on Skype, they have the potential to see your entire contact list. Here's how:

1. Create a new alias account on skype.com with an empty contact list (very important). You don't need to install Skype.
2. Search and add your target. They have to accept your invitation for this to work.
3. Now when you search for someone in the search bar, e.g. you type "a", a dropdown of potential hits will start to populate as you type. On the top of that list, Skype will always have accounts that say "1 mutual connection". Since you don't have any other contacts, this means that the suggested user is in your target's contact list. Type "b", and any user that is in your

target's contact list with "b" in their username will show up.

4. Cycle through all the letters of the alphabet to reveal every contact in the search field that says "1 mutual connection". Write them down.
5. In under 10 minutes you will know your target's entire contact list (unless they have thousands).

This may be a feature of convenience by Skype, but this is definitely a privacy flaw. Mitigation? If you're on Skype, don't accept an invite from anyone you don't know and expect.

"Puzzles" by Anonymous:

Your crossword puzzles are too easy and are not fun. Make them more complicated for those of us who have an education.

Editor's Note: We are all excited to see your crossword puzzle contribution for July! You are going to make it better, right? ■

ANDROID SANITIZATION PACKAGE NAMES

By Anonymous

This is in the context of the Privacy, Security, & OSINT Show, Episode 246-Android Sanitization, which can be found here:

<https://inteltechniques.com/blog/2022/01/14/the-privacy-security-osint-show-episode-246/>

Android sanitization offers privacy enthusiasts a scalability of private mobile device options. This is exceedingly useful when helping friends and loved ones who are sympathetic to privacy, but not ready to jump onto the GrapheneOS train. However, the privacy enthusiast can encounter some snags while sanitizing an Android device. One difficulty I encountered when utilizing the Android Debugging Bridge (ADB) tools with an Android phone, was that the uninstall command requires knowing the Android package name of the application you want to uninstall (such as "com.android.vending" for the Google Store application).

Using the list command with a grep query helps with this when part of the app's label is included in its package name. However, some applications have a different label and package name. One example I encountered on an old Pixel was the SIM Manager app, which has the package name "com.google.android.euicc". This package name cannot be located using grep queries of "SIM", "Manager", or "SIM Manager".

Some APK hosting websites can help with this problem by searching for the app label. However, some of the more obscure stock applications can't be found on APK hosting sites. Another option is that there are also apps that, once installed, can display package names of other installed applications. However, if you have been following the IntelTechniques privacy strategy, you likely already have the tools you need to fulfill this function installed on your Android device, negating the need to install an unvetted application.

This leads to the solution that I have found: finding package names using the Aurora Store. Here's how: open the Aurora Store. Open the menu in the upper left. Select "My apps & games". Select the desired application, in this case the SIM Manager application. Open the kebab menu in the upper right. Select "Manual download"—we will only be viewing this menu, and not actually using the manual download function. Under the manual download menu, you will see the package name listed under the app label; in this case, the package name is "com.google.android.euicc".

There are many advantages to this technique. One is that it doesn't require the package name to match the app label. Another is that it accounts for obscure stock applications that might not be listed by APK hosting websites. Finally, it utilizes a tool that we already use as part of the private Android and custom ROM strategy, rather than relying on some new tool that might not be compatible with our threat model. ■

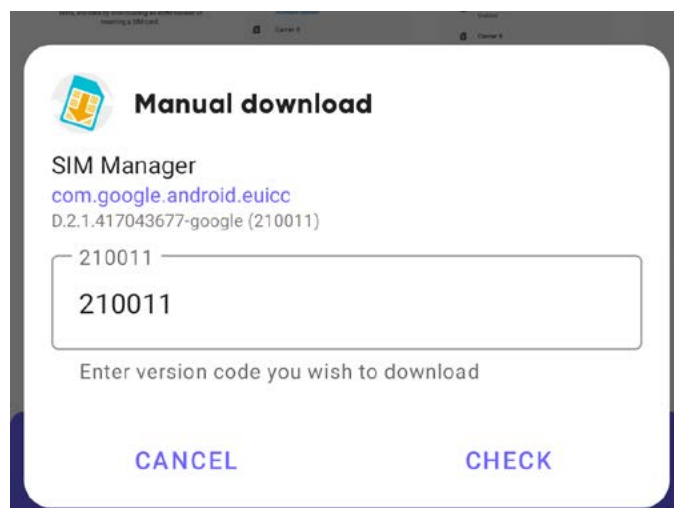
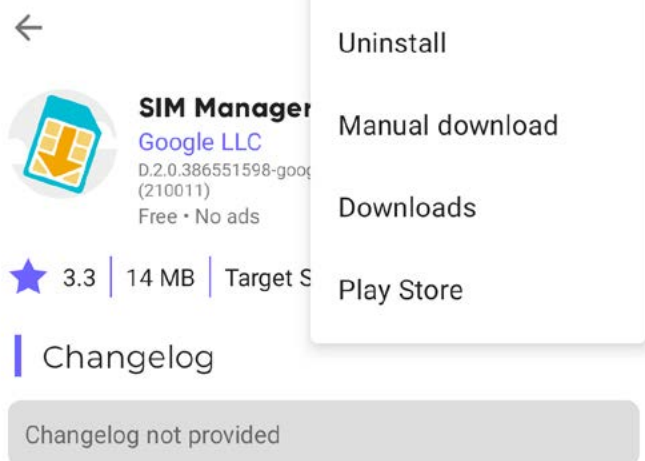




Image: Jonathan

MY SECRET LITTLE DIGITAL WORLD

By Digitally Semi-Anonymous

I want to share some content about my continued privacy journey. I'm a social guy by nature, I use social media, and I don't take myself too seriously. I generally listen to podcasts hosted by comedians, and wanted to listen to something different. I started searching for technology type podcasts and came across Darknet Diaries. The specific episode I listened to that caught my curiosity was on OSINT! I was hooked on the idea immediately. I had a feeling of being a kid again, that thought of maybe seeing or finding something I wasn't supposed to. Something I knew of but others didn't. So I started googling all things OSINT, but I didn't really understand what I was looking for.

I searched podcasts for OSINT. That's when I found MB. This podcast completely changed how I think, how I manage my digital life, and I have learned so much. I will be forever grateful for what it, its guests and experiences, offer to us, the listeners. I gravitated more towards the privacy & security side, but appreciate the OSINT part as it justifies the privacy. After trying out all the recommended

services and understanding how to use them, I wanted to share with other people what I had learned and help others protect their digital life. I was perplexed by the resistance.

I was met with "What do I have to hide?", "I have nothing to hide." and "You want me to download a what?". Not my wife, friends or co-workers showed interest. I provided a very strong case for some basics like a password manager, VPN, firewalls and planting your flags. They would all say, "Oh wow, my login credentials are out there?! Oh well, what can I do..." I quickly realized that this was a solo adventure.

I spoke with my wife on multiple occasions about her digital privacy and security, but she wasn't having it. I have since made a small crack in that foundation of "I want no part of this". Just a few months back we were throwing out some attic items we no longer needed. One specific item was her old suitcase. I asked her if she wanted to keep the decorative tag on it which had her name and address. She says no. As I'm walking it out to my truck, she says "Wait, where are you going?". I replied "You said you don't

want this". She says "I don't, but take my tag off of it".

I stop dead in my tracks, drop the suitcase and slowly turn around with a huge grin on my face. At that moment she knew exactly where the conversation was going. I very sarcastically asked, why would YOU care if your name is on this? I'm throwing it into a dumpster at the landfill. She says I don't want some creep seeing it and knowing where to find me. I walked up to her, put my arms around her and explained that this feeling you have in this moment, is why I spent many hours removing our info from all these people search websites. All the things I try to explain to you about my "secret little digital world" as she calls it, is for our protection and well-being.

This was the perfect moment to once again pitch Bitwarden to her. She now uses Bitwarden. She also has a daily routine of doing different puzzles on her iPhone. I would cringe when I saw this, because I know what's happening in the background as its sucking up everything she's doing. One day we were talking, and she mentioned an item that kept popping up in ads that she had searched for, and she

was finding it annoying. Another opportunity presented itself, and I hit her with the iOS firewall app Lockdown. I pitched it, she reluctantly downloaded it, but is still using it to date. I check it now and again, and it blocks about 10k-15k callbacks to the mother ship a day, and is currently at 1.75 million total blocks. She turns it off for one puzzle app because Lockdown completely shuts it down, but she does turn it back on, something I would claim as a small victory for our privacy. Whether she likes Bitwarden and Lockdown or not, she is using these services.

Every now and again we spoil ourselves at a nice steak house. They require a credit card to hold the reservation and charge you \$100 if you cancel within 24 hours of the reservation. In life, things happen. Maybe you get in a fender bender on the way or a flat tire, or maybe you, or someone you're taking, becomes sick hours before your dinner reservation. From now on when we make a reservation, I explained that we will be using a Privacy.com card to protect us from those fees if an unforeseen circumstance pops up. My hope is that she will see the value in it, and when she does, I will be waiting in the shadows for my opportunity to spring it on her to create her own account.

The moment I realized how important our digital privacy is, was when I received an email from Venmo. I couldn't even remember setting up an account. I was curious, so I tried logging in, and due to previously poor password recycling, I got in. I had never actually connected it to a financial account, but created a profile. At the time, I think Venmo made your profile public, and you had to change it to private, otherwise anyone could see your transactions. Upon logging in, I saw all my contacts' accounts and their transactions. I could click away from one individual to the next to the next and so on. I could randomly search for people and saw way more than I thought I should see, which included a friend of mine's fiancé, whose best friend was a local Chief of Police. I could keep clicking, and noticed transactions to other police

officers. I was blown away. That was the moment I started taking my privacy journey more seriously than just a neat new thing. I deleted that account, and a few months later I saw an article that talked about how Venmo was making some changes due to privacy concerns.

I would like to share a few things that help me in my privacy journey, and it may help you. My four social media apps are on an old Wi-Fi-only device that is used only for that purpose. Nothing else is searched for, logged into, it has a different Apple ID, ProtonVPN and Lockdown with added custom domains to block. I'm not overly concerned about what it might be collecting, but with Facebook specifically, most users use their real name. Shorten your name, use initials or change it just enough. That way, if someone is trying to find you on Facebook, it's less likely they will, as they are probably searching for your real name. Also, go through every setting in each account to reduce your exposure, and always use 2FA where available.

You also have the ability to change your caller ID with your cellular carrier. When my caller ID pops up, it is not my real name, nor is it my alias. Some telephone number search sites query your cellular number to the legal name used at sign up to do a credit pull. This is separate from your caller ID. You can change this, but can't leave it blank. My carrier (AT&T) doesn't allow the use of special characters for a name, so I use a single initial for first & last name. They are not my actual initials, so if a search site queries my number through an API, it shouldn't be too revealing if this is a site you're unable to completely opt out of.

My mailman threw me a curveball a few weeks ago. She knows I get some bills in my alias name, many Amazon/USPS packages are delivered to this mystery person she has never seen. Sometimes she asks if I have let "alias" out of the basement yet. I always tell her "And risk getting caught? No way!". I wasn't home, and she left a sticker for a package my alias had to sign for. I met up with her down the street to get my package. She says "Oh no, you can't

sign for this, alias has to sign for it". I paused like a deer in the headlights. I hadn't fully thought this through and was caught off guard. She stood there smiling waiting to see my reaction. All I had was "Alias is sick with COVID and asked me to sign for it". I signed my real name, as I have never written out my alias name before, and it's probably illegal. Don't be caught off guard like I was.

I'm a ProtonMail and Bitwarden subscriber. Another thing I do is I use the same email address to log into these 2 accounts. That email address is not forwarded to, not used to sign in anywhere else on the internet or receive email except from those services. So the likelihood of that login credential being discovered or breached is very low. Even so, both logins are protected with 2FA so I'm not overly concerned. My ProtonMail account has multiple emails created and ready to go in the event I need to provide a new address in an urgent situation. They are currently disabled and have not entered the online world. I suggest taking advantage of all the additional free ProtonMail addresses they offer to paid subscribers when they introduce a new @domain address.

Being a delivery guy I hear store patrons everyday giving their phone numbers to store employees to associate their account with the purchase in order to get points or discounts. This community understands how dangerous this action could be. You never know who is listening or what a bad actor might do with the info you just gave out for everyone in earshot to hear. A very targeted phishing attack could be played out shortly after the purchase making it seem legit, and then be taken to the cleaners or lose access to online accounts. This is where I use a screenshot of my account's barcode in my alias name that is saved in my iOS Files app, because I, too, want that discount, but without exposing my info or having a privacy invasive app on my device.

Be vigilant, be smart and be well. ■

WI-FI GEOLOCATION CONCERNS

By Privacy Mike

One day when auditing my online account security, I noticed Microsoft knew exactly where I lived, down to a few feet, within my large apartment complex. For most, this would be an unsurprising finding. However, I subscribe to most of the extreme privacy techniques, and this caused alarm.

My home network uses a cable modem attached to a Protectli firewall that then attaches to a Wi-Fi router. My Protectli box runs pfSense which creates an always-on VPN connection, with a kill switch preventing any traffic from leaving my network unless it's on that VPN.

I don't have any cell phones inside my home. I use a prepaid phone, paid in cash, that never leaves a faraday bag when within a few miles of my apartment. I don't have any GPS devices inside my home.

Yet, there it was, on my Xbox's Account Settings page. A picture of a map of my apartment complex, with a pin located exactly where I live, as the last login location.

This was a few years ago, and I struggled in figuring out how Microsoft was doing this. No one was talking about this, and even today few discuss it. I uncovered the technique of Wi-Fi beacon tracking.

My Xbox is not allowed to touch the internet without first going through a VPN. This means Microsoft does not know my home IP address, and could

not be identifying my location through those means. However, all modern Xboxes have Wi-Fi network cards built in. It's how most people connect their Xbox to the internet, and it's how the wireless controllers communicate with the console.

First, a bit of background on how Wi-Fi works. All Wi-Fi devices have a unique MAC address that identifies the device. No two devices have the same MAC address, because different companies have different prefix codes, and each company can ensure their own devices that follow their prefix code have a unique serial number.

Wi-Fi devices are constantly looking for other Wi-Fi devices. A Wi-Fi device with nothing to talk to is useless. So the core tech relies on seeing all other devices around it for potential connections.

I hardwire my Xbox to my router. But, I can't "disable" Wi-Fi because it's part of how the wireless controllers work. Even if I got a wired controller (and good luck finding one in 2022), it's likely impossible to tell the Xbox operating system to disable Wi-Fi completely.

And this is because Microsoft doesn't want to let you disable Wi-Fi. Like all of the big tech companies, Microsoft is a data hog. It wants to know all of the things. Like, for example, what other Wi-Fi devices exist in close proximity to your Xbox.

What I figured out is that my Xbox is seeing my neighbor's Wi-Fi routers. Of course, I know it "can" see them, because anytime I enable Wi-Fi on any

of my devices, I see a list of a few dozen of my neighbor's Wi-Fi routers. But what I didn't know was that Microsoft then collects the information about which nearby routers it "sees" and reports it back to Mr. Gates' headquarters.

My neighbors likely do not run 24/7 firewalls, and thus Microsoft has associated actual geographic locations with my neighbor's Wi-Fi router MAC addresses. Thus, by virtue of my Xbox seeing signal strengths from these dozens of Wi-Fi routers, Microsoft can estimate where my location is down to a few feet using trilateration methods.

I dug into this further and learned that the various companies that send cars with cameras around to map city streets, such as Google Street View, are not only collecting pictures of everything, but also "wardriving" MAC addresses of every Wi-Fi router they see, and log it along with the GPS location and signal strength of that router.

It's not necessary to send cars around to do this. Apple and Google have cell phones with built-in GPS in 99.99% of households. Even if you're running a full network VPN, the phone can see your neighbor's MAC addresses, as well as your own router MAC address, and report it back along with the GPS stamp, giving away your true location.

This does not render always-on VPNs useless. There is still protection in the form of websites you visit not knowing your home location and preventing your ISP from logging all of your web traffic history. However, it does mean your geographic location is trivial to

determine if you live anywhere with neighbors' Wi-Fi signals accessible in your home.

Even if you don't live in a populated place, and you invite someone over to your home who has a cell phone in their pocket, their phone will sniff your Wi-Fi MAC address, "tag" it with the GPS coordinates of your home, and send that back to their database. The visitor doesn't even need to have your Wi-Fi password or connect to your Wi-Fi to do this. It will happen automatically without your visitor's knowledge, because Wi-Fi devices are constantly sniffing and recording all of the other Wi-Fi devices they see.

I've come up with a few means to reduce the threat. First, if you live in a rural place without neighbors, then have a means to quickly disable Wi-Fi in case you have a guest or a tradesman come to the house. Reduce the Wi-Fi signal strength and install a fence so it's not possible to sniff from cars driving past the home.

Even this won't be a 100% solution, because it only takes a single instance of another person's Wi-Fi device to

see your home router MAC address to make that permanent linkage to the location. From that point forward, every time you connect a device to your router, then Apple, Google, Microsoft, etc., will associate that device with your true location.

Completely eliminating all Wi-Fi would be the only true way to get rid of this threat. It's a big commitment, because not only do you have to hardwire ethernet cables everywhere and manually plug in devices each time you want to connect to the internet, but you'd have to physically remove Wi-Fi network cards from every device you have.

Back to the Xbox. It's not enough for me to "tell" Xbox not to use Wi-Fi. I'd have to open the Xbox and physically disconnect the Wi-Fi card. This likely will require desoldering and may brick the device if the startup routine checks for functioning Wi-Fi during the boot cycle.

One method I have not tried, but suspect will work, is living in a rural area and buying several different Wi-Fi routers that I spread throughout my

home. I perform my own "wardriving" of a neighborhood that I would like to pretend I live in, and document the MAC addresses of several routers in one apartment complex of that place.

I then install new firmware onto my own routers and overwrite their MAC addresses with those of the routers I identified during my wardriving effort. I also name each router's network the same. When I turn my Xbox on, it will "see" these five routers nearby and report the network name and MAC address back to Microsoft who checks their database and estimates that I live in an apartment complex that's a hundred miles away from where I really am.

I considered doing this as an experiment, seeing if Microsoft would be fooled, and presenting the results at a conference, however I value my privacy too much to do that, so if anyone wants to build off my theory and present it at DEF CON, go ahead.



SimpleLogin

Receive & send emails

anonymously

With email aliases, you can be anonymous online and **protect your inbox against spams and phishing.**

simplelogin.io

1. Use email alias **everywhere**

EMAIL ADDRESS GENERATOR

Alias-email@simplelogin.com



2. Receive emails **safely in your inbox**

★ Dad

★ Facebook

via SimpleLogin

★ Buddy



3. Send emails **anonymously**

FROM Alias-email@simplelogin.com

TO Facebook Support

CAN DECENTRALIZED IDENTITY GIVE YOU GREATER CONTROL OF YOUR ONLINE IDENTITY?

By Dr. Paul Ashley,
Anonymo Labs

Over the past year or so, interest in decentralized identity (also called self-sovereign identity) has surged. We've seen new decentralized identity blockchains created, decentralized identity companies acquired, and various real-world decentralized identity-based projects progressed.

You might ask then, what is decentralized identity? Definitions vary, but this is a good one:

Decentralized identity is an approach to identity and access management (IAM) that seeks ways to allow individuals to manage their own personally identifiable information (PII) instead of using a central authority. An important goal of decentralized identity is to create standards that will allow internet users to control which applications and services can have access to specific types of PII.

Let's break it down. This definition has three important concepts:

1. Identity and access management (IAM)
2. User control of their personal information (PII)
3. Standards

Identity and access management (IAM) refers to the way you access an online service, such as a website or social media site. The first type of IAM model implemented, and the most common, is *centralized*. We all know this approach, since it involves creating an account on a service. Typically, when you create an account you give the site a username, password, perhaps set up two-factor authentication (2FA), and give other personal information such

as your mobile phone number, email address, and credit card information. When I look into my own 1Password app, I see I have more than 200 accounts that fit this model.

The second type of IAM model implemented is also a centralized model, but is called *federated*. In a federated model, you create an account at a central site, such as Google, Facebook, Twitter, LinkedIn or one of the other big sites. When you go to other websites, you might be offered the option of doing a social login such as "Login with Facebook", where you use your Facebook login to access the third-party site. This type of model relies on sophisticated *federation protocols* such as OpenIDConnect. The advantage for you is convenience.

Decentralized identity flips these centralized IAM models on their head. With decentralized identity technology, instead of entering a username and password or doing a social login, you would **create your own identity in an identity wallet**. You would bring that identity to the website or service and create a peer (also called a pairwise) connection with that service. The advantage of creating the connection is that it allows for end-to-end encrypted communication, strong authentication and so on.

Now let's consider the second part of the definition: **user control of their personal information (PII)**. In my view, the two centralized IAM models are designed to behave exactly opposite to this goal. Those models encourage you to disclose as much of your personal information as possible, and collect even more by surveilling your activities covertly. This is particularly bad with social login, where you are actually helping the central site (e.g. Google)

to get a broader view of your behavior. While it's tempting to hit the social login button to save the bother of creating yet another account and remembering or storing yet another username and password, when you do, you're really *trading* your personal information for access and convenience. Unless you carefully consider and agree to the information that the third-party site is asking to access from your social profile (during the initial permissions process, which many people rush through), you can easily expose your personal data, including your gender, age, email address, phone number, relationship status, interests, and even your full list of connections. Almost everything you've put into your social accounts could be available to the third-party site owner. This obviously has privacy and security implications.

So decentralized identity also flips this broad-ranging data gathering on its head. With decentralized identity technology, you would initially disclose one of your decentralized identifiers (DIDs) to the service to set up a connection. This allows the service to identify you for subsequent accesses and authenticate you using public key cryptography. You no longer need a password. **You then negotiate with the service what additional personal information you consent to give to the service.** Technology called verifiable credentials (digital documents issued with digital signatures) makes this possible.

Let's now look at the third important concept in the definition: **standards**. Arguably the most important goal of the decentralized identity community is to define a set of standards to allow interoperability for users and services—essentially, an interoperable decentralized identity ecosystem.

The standards being defined are at standards bodies such as World Wide Web Consortium (W3C), Linux Foundation (Hyperledger and TrustoverIP), and Decentralized Identity Foundation (DIF).

Now we have touched on the high level concepts, let's dig a bit deeper into the decentralized identity technology.

Identity wallet

As the user, your view into decentralized identity is via an identity wallet. The wallet allows you to create your decentralized identities and connections with other users and services, and to receive, hold and present verifiable credentials (your digitally signed digital documents).

First, you need to get an identity wallet. There are a few different ones out there; one example is the Lissi wallet (lissi.id/mobile), which is a mobile application purposely built to allow the user to participate in a decentralized identity world.

The wallet is designed to hide much of the complexity of decentralized identity, but let's cover some detail here. When you create your first decentralized identity, you are in fact creating a private/public key pair (usually based on Elliptic Curves, e.g. ec25519) and a unique identifier called a DID. A DID is a simple text string consisting of multiple parts:

```
did:indy:sovrin:7Tqg6BwSSWapx-  
gUDm9KKgg
```

The string above has this meaning: "I am creating my decentralized identity following the Indy DID method, and the identity is anchored on the Sovrin

mainnet blockchain." If you were to provide that DID to a service or another user, it would be resolvable to an address on the Sovrin mainnet where the DIDDoc could be returned. The DIDDoc contains your public key and an address where to reach you.

There is a lot to unpack in that paragraph.

Sovrin is a Hyperledger Indy-based blockchain specifically built for decentralized identity. Being a permissioned blockchain, it is a network of validator nodes (twenty four for each of the three Sovrin networks: mainnet, staging, test). It is designed to support decentralized identity-based applications. Anonymo Labs is one of the founding stewards of Sovrin, meaning we have been running a validator node on the Sovrin network for over three years now. Think of a validator like a bitcoin miner.

A blockchain is used for decentralized identity because it provides an anchor for trust. Not only can you write your DIDs to the blockchain, but other parties, such as verifiable credential issuers, can write credentials definitions and their own DIDs (unique identifiers) as well. Because the blockchain is immutable (can never be altered, only added to), there is no way for a hacker to modify the information on the blockchain.

DIDDoc is also important. The DID points to a location on a blockchain so that a DIDDoc can be retrieved. The DIDDoc gives the decentralized identity's public key (for establishing connections) and an address that can be used to reach you as the user.

A well-designed identity wallet shields you from the complex technical information I've described. From your perspective, you create your decentralized identity and take it out and use it. Complexities around cryptography, endpoints, and blockchains are not that interesting to the everyday user.

So, to answer the question we started with: can decentralized identity give you greater control of your online identity? Clearly yes.

I'll leave it there for now. This is the first in a series of articles on decentralized identity from Anonymo Labs. In future articles I'll discuss:

- Decentralized identity focused blockchains
- Decentralized identity verifiable credentials
- Identity (data) hub concept
- Real world projects leveraging decentralized identity
- The key decentralized identity standards, and more. ■

Made you look!

Want to support this free magazine? We'd love it if you sponsored us by promoting your product or service with a full-page, half-page, or quarter-page ad!

Don't have an ad design? Our partners at Astropost would love to build you an awesome, magazine-ready ad!

Click this banner or go to UNREDACTEDmagazine.com for details.

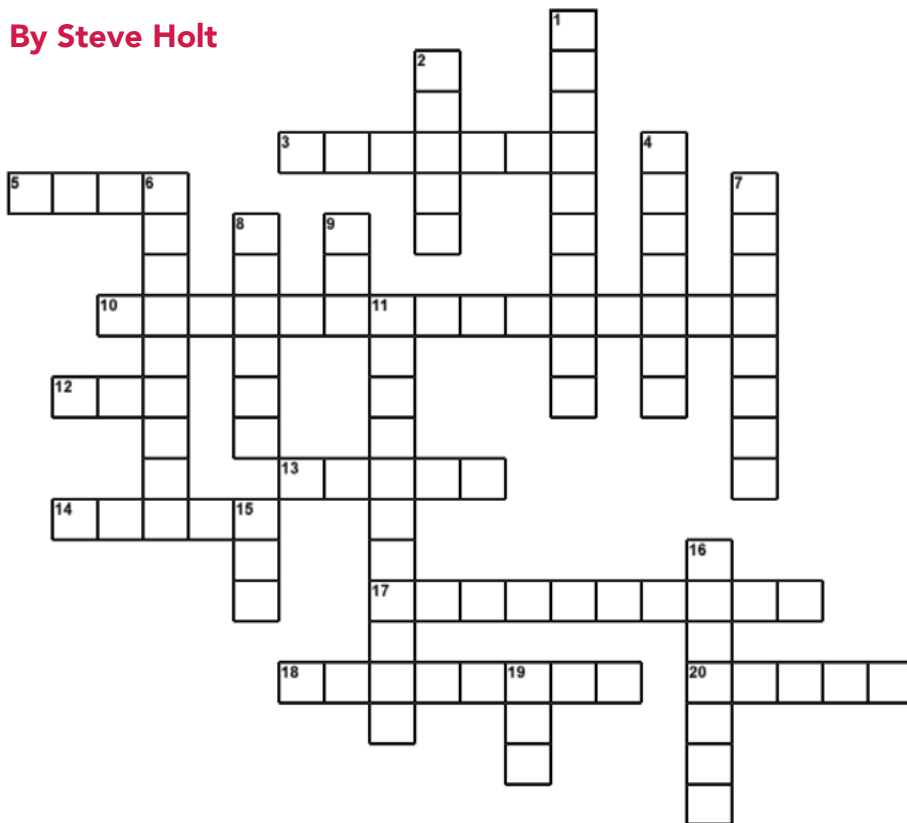


Astropost

UNREDACTED
THE PRIVACY, SECURITY, & OSINT MAGAZINE

PRIVACY-THEMED PUZZLES

By Steve Holt



Across:

- 3. Hardware 2FA token
- 5. _____ mining
- 10. Resource for tools, training, & certification
- 12. Physical cellular card
- 13. Tux
- 14. Operational Security acronym
- 17. Digital extortion
- 18. MacOS 12.3
- 20. Secure browsing protocol

Down:

- 1. Android emulator
- 2. Fake name
- 4. Copies of data
- 6. Cash is king for _____ payment
- 7. Email trickery scam
- 8. Elliot Alderson's pet fish name
- 9. Billions of connected devices, abbr.
- 11. Social _____
- 15. Computer security game, abbr.
- 16. Records vehicle activity
- 19. _____ team

The answers to the crossword puzzle can be found within the word search to the right and on the following page.

Editor's Note: We are always looking for privacy-themed puzzles, including crosswords, word finds, and anything else you might create. Send us your best submission for next month's issue.

B	I	J	Y	B	W	I	P	W	A	R	R	R	D	H	B	N	Z	F	P
C	O	E	W	S	S	L	D	J	W	A	L	I	A	S	K	C	B	M	B
R	Y	G	B	H	K	U	R	B	T	E	E	I	S	E	I	Z	W	F	K
D	P	A	E	T	J	R	B	G	P	H	I	S	H	I	N	G	M	I	F
J	Z	P	L	K	Y	S	D	H	P	T	U	I	C	U	T	Y	G	M	R
W	P	J	C	M	J	R	A	N	S	O	M	W	A	R	E	E	O	N	K
R	M	H	G	Z	S	T	T	R	O	D	K	K	M	P	L	I	N	U	X
K	N	Y	Z	O	F	B	A	F	J	B	P	J	G	F	T	F	I	I	L
B	S	B	W	B	D	E	W	R	Y	U	N	L	Q	W	E	R	T	Y	G
W	Y	W	K	R	M	L	L	F	U	E	H	U	W	N	C	D	U	G	J
N	D	G	S	D	R	H	A	M	B	M	G	N	U	Z	H	F	P	S	U
H	O	N	G	I	F	E	N	G	I	N	E	E	R	I	N	G	P	C	G
C	S	A	Z	Z	O	P	O	B	K	Y	N	F	Y	P	I	M	Z	A	I
W	I	L	D	R	D	K	N	N	E	G	Y	F	T	S	Q	L	Y	Z	C
M	O	N	T	E	R	E	Y	T	Y	C	M	A	H	S	U	M	J	B	A
C	T	G	O	D	T	E	M	I	B	I	O	S	T	O	E	J	D	B	E
Z	P	Y	F	L	H	M	O	G	K	M	T	R	T	K	S	Y	Y	S	B
B	B	R	B	A	C	K	U	P	S	S	I	K	P	S	S	W	J	H	A
D	Y	T	P	Y	T	N	S	I	I	D	O	P	S	E	C	R	A	P	K
S	A	K	O	I	F	E	F	K	M	T	N	D	N	U	N	G	S	Y	B

FINAL THOUGHTS

By Michael Bazzell

I am already thinking about the July issue. While I have a few articles brewing in my head, this magazine cannot be completed without you. Please send your contributions sooner rather than later if you would like to be published within the next issue. I sincerely thank everyone who contributed to this second release. I look forward to seeing what you come up with next.

~MB

CROSSWORD ANSWERS

Across
3. Yubik
5. Data
10. IntelTechniques
12. SIM
13. Linux
14. OPSEC
17. Ransomware
18. Monterey
20. HTTPS

Down
1. Genyotion
2. Alias
4. Backups
6. Anonymous
7. Phishing
8. qwert
9. IoT
11. Engineering
15. CTF
16. Dashcam
19. Red

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>

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

PIA Dedicated IP VPN Service: <https://www.privateinternetaccess.com/ThePSOSHOW>

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

Fastmail Business Email: <https://ref.fm/u14547153>

SimpleLogin Masked Email: <https://simplelogin.io/?slref=osint>

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

VARIANT DETECTED.

Websites and graphics.
For businesses who
respect privacy.

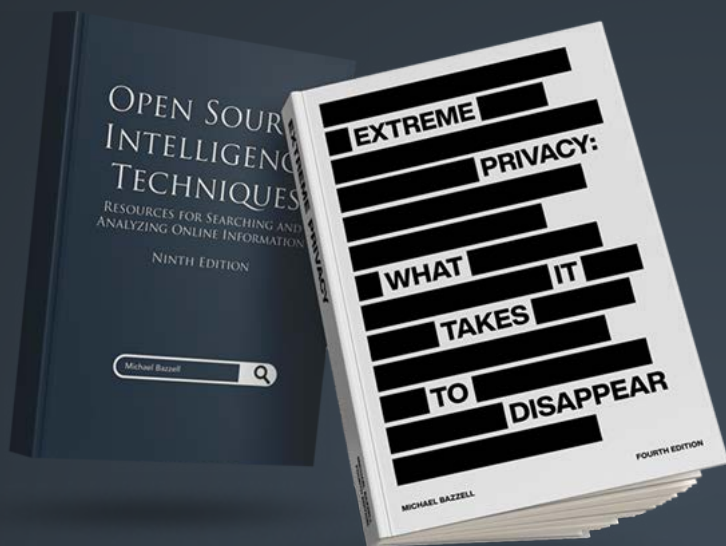
Be a variant.



Astropost

Astropost is the official design partner for this issue of UNREDACTED MAGAZINE. Need an ad designed for the magazine? We'd love to help you out!

New 2022 Privacy & OSINT Books



- ✓ Hardcover & Paperback
- ✓ New & Updated Content
- ✓ 500+ Pages Each @ 8.5 x 11
- ✓ Our Full Playbooks
- ✓ Supports This Free Magazine

Order at IntelTechniques.com

OSINT & Privacy Video Training

90+ Hours of Video Training | Optional OSIP Certification

Register at IntelTechniques.net

