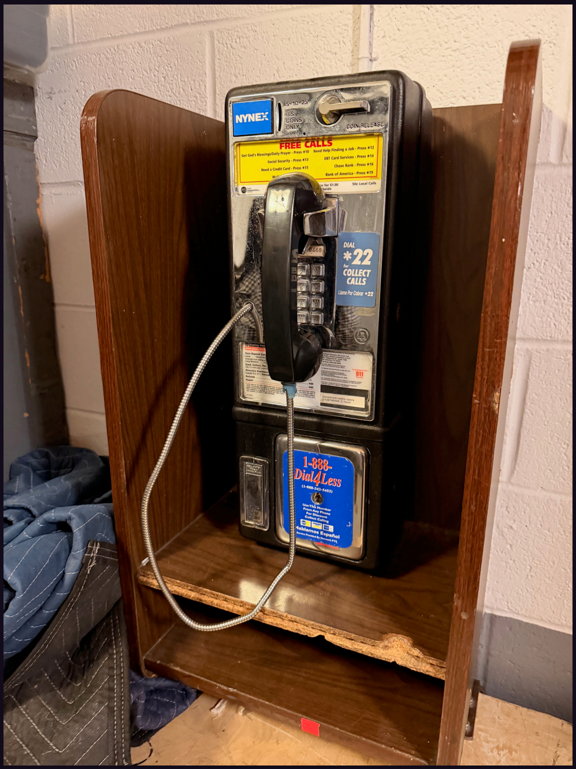
Volume Forty-Two, Number Four

DIGITAL EDITION Winter 2025-2026

2600

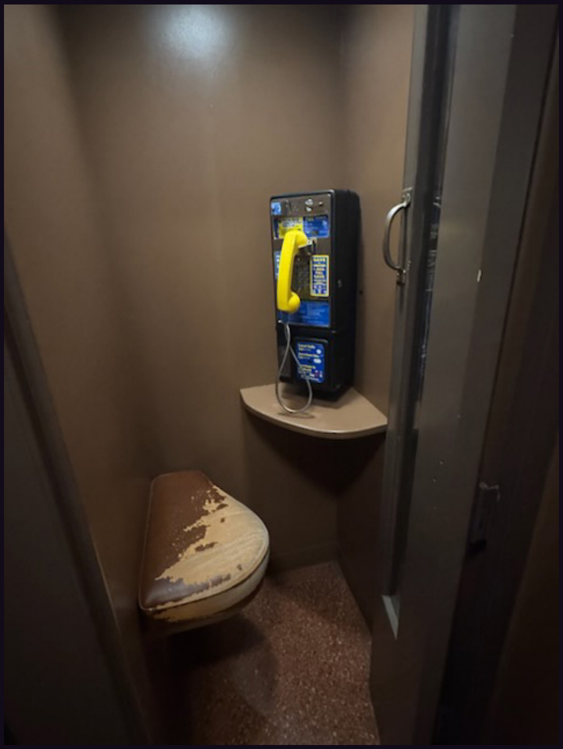
The Hacker Quarterly

Hidden Payphones



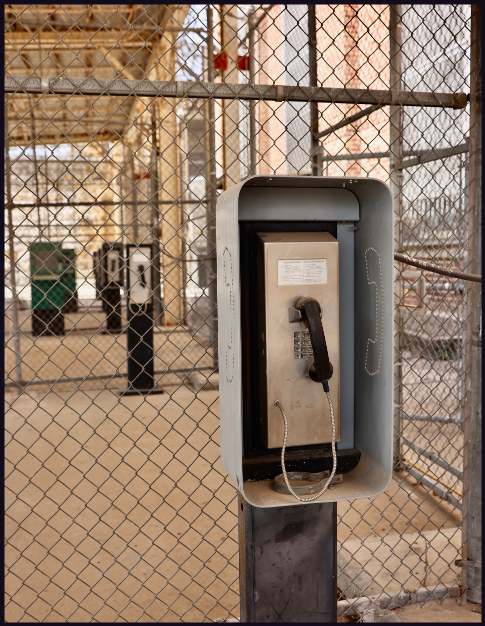
The Metropolitan Opera. This is the one surviving payphone in the lowest floor in the basement below the stage. It is sadly not operational, but there's a penny in the change slot and everyone has made a silent agreement to leave it there.

Photo by Harlan Haskins



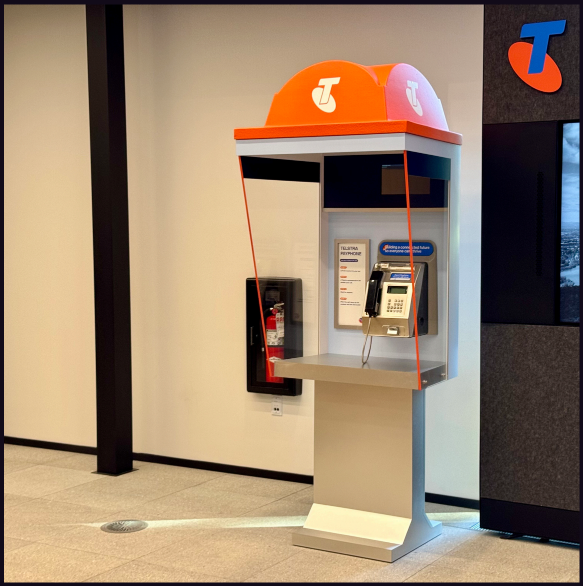
Radio City Music Hall. If you can find your way into the men's lounge on the second floor, you'll find this phone and an entire booth from the past. A true New York City time capsule.

Photo by Michael Wild



Lansing Correctional Facility. Operated by the Kansas Department of Corrections, these phones are in a part of the prison that opened in 1868 and closed in 2019. Inmates paid from their prison accounts to use these phones.

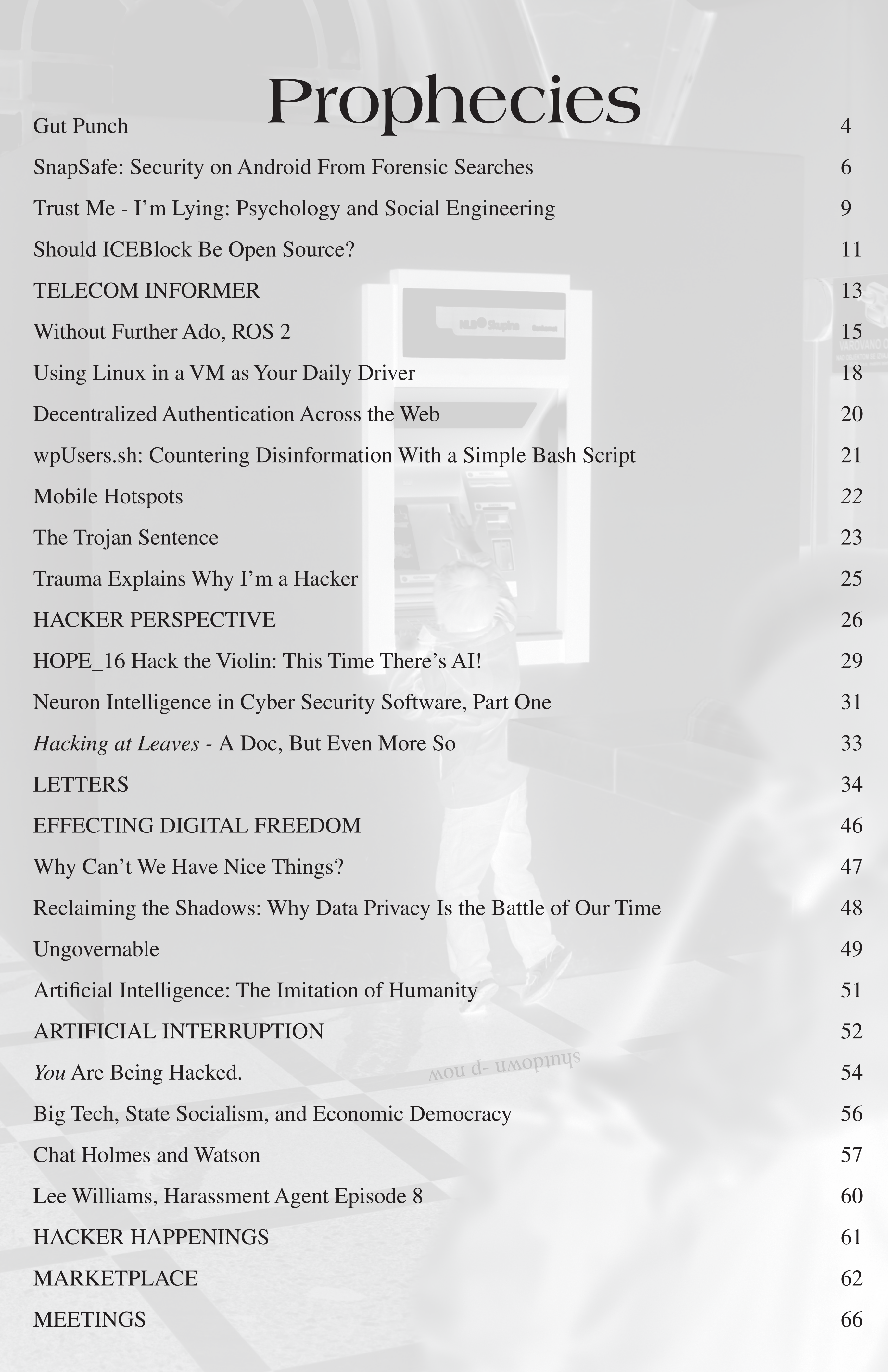
Photo by Sigo31



Microsoft. This Telstra payphone is installed in Building One of the East Campus in Redmond, Washington. It's within the invite-only Experience Center One, so it might be difficult to ask them why they have an Australian payphone there.

Photo by Duck Duck

Got foreign payphone photos for us? Email them to payphones@2600.com.
Use the highest quality settings on your digital camera! (Do not send us links as photos must be previously unpublished.) (more photos on inside back cover)



Prophecies

Gut Punch

We did not see this one coming.

It's really quite amazing how much we've been through over the years with HOPE. Our Hackers On Planet Earth conference has always been full of surprises and challenges. We strove for edgy content and an inclusive atmosphere. We got all of that and more. Nobody wanted to stop.

Then COVID hit in 2020. Our hotel was torn down in the years after. Finding another hotel in the area proved to be impossible. So we shifted gears and wound up at St. John's University in the neighboring New York City borough of Queens. We didn't regain the full attendance, but we were thrilled at the extra space a college campus offered, not to mention modern, working equipment. And the content remained every bit as good.

It was definitely different. But, as hackers, we tend to make different work.

The bad news came this autumn when we were told that an offensive pamphlet at HOPE_16 in August had gotten the attention of the university president's office. The matter was "carefully reviewed internally" without a word to us and they came to the conclusion that HOPE should no longer be allowed to take place at St. John's.

We've had plenty of controversial material over the years in one form or another - content, images, speakers, etc. But every time there was a concern with a venue, we were contacted and consulted. And each time, we were able to come to an understanding and, if necessary, take action that we were comfortable with to resolve the situation. Not once did anyone dictate what we couldn't do or say at our speaker presentations, workshops, or performances. We never would have tolerated that.

It's painful to realize that a college campus - where freedom of expression is supposed to be encouraged and celebrated - no longer appears to value this very basic premise. We've seen many examples lately of universities acting in panic to avoid being punished by an administration that is often quite hostile towards higher education. We're not saying this is necessarily what happened here. But the lack of communication and the way this all played out makes it difficult to come to another conclusion.

The letter we were sent claims that "some of the materials and messaging" at HOPE "were not in alignment with the mission, values, and reputation of St. John's University." This is an incredibly vague statement that could be applied to almost anything. We constantly question authority, look for ways to defeat restrictions, and encourage a spirit of peaceful rebellion. The very existence of HOPE could be the wrong messaging in the eyes of someone who doesn't get what we're all about. We were eventually told the actual reason was the title of a pamphlet that was on a table which was interpreted as being "anti-police."

Several things: 1) The pamphlet in question was something an attendee had brought which was not part of the conference program. 2) People are allowed to be anti-police. It seems bizarre to shut down an entire conference because an attendee has a controversial opinion. 3) There was no attempt made to discuss or address this. Someone with an obvious ulterior motive quietly took a picture of the pamphlet and reported it to the president's office after the conference had ended. 4) The offending phrase on the pamphlet ("Fuck tha Police") is actually the title of an N.W.A. song that was recently ranked by *Rolling Stone* as Number 10 in "The 100 Best Protest Songs of All Time" and Number 190 in the "500 Greatest Songs of *All* Time." According to Wikipedia, these words "continue to influence popular culture in the form of t-shirts, artwork, political expression, and has transitioned into other genres as seen in the cover versions by Bone Thugs-n-Harmony, Dope, Rage Against the Machine, and Kottonmouth Kings." Far from an ignorant and offensive phrase, these words actually are quite significant and represent a good bit more than might be obvious at first glance. (And even if they didn't, the reaction to them was completely out of proportion.) 5) Not one person had complained to any of the HOPE staff about this or any other offensive content. It doesn't mean everyone agreed with everything they saw or heard. It means they didn't see it as an issue that affected the conference adversely. 6) We got along great with everyone involved in law enforcement who was at or around the event and the feeling was mutual. There was even a mass graduation of police cadets on the first day that received well wishes from many of our attendees.

We know this decision doesn't represent most of the St. John's community, who we've enjoyed working with greatly for the three conferences we've had there. And we don't believe the fact that it's a religious institution was a factor here, as some have suggested. As mentioned, we've been seeing disturbing trends of this nature at a number of universities. In the end, St. John's has the right to decide who they allow on their campus. We believe they made a big mistake here, as our attendees did nothing but add to their reputation and significance in the world of high tech. Everyone from university liaisons to members of the security team to custodians to students had high praise for the unique individuals we brought to their campus. Those relationships will now go no further and it's a loss for all of us.

So what's next? Yet again, we find ourselves at a turning point.

We had originally scheduled HOPE 26 for next August at St. John's. Since that won't be happening, we've been looking into other possibilities. There will be more updated information at either hope.net or 2600.com. But we must also decide what we want to do for the long term. We've had a pandemic, hotel destruction, and now eviction get in the way of our events in just the last six years. Far from giving up, we intend to keep looking for a solution that will let HOPE not only survive, but prosper. That's the intent. But whether or not we actually achieve that is very much dependent on if enough people come forward and help that happen.

We've long held a belief that every time we get knocked down, we come back stronger. The outpouring of support so far has been quite inspiring. We are determined to do whatever it takes to make this event happen and for it to continue to be as significant and inspiring as it's become. Giving up just isn't an option.

***

Greg Newby was the best of us. In the decades where he was involved with HOPE and *2600*, he never stopped trying to make things better. Ironically, it was he who discovered St. John's as a location for HOPE after we lost the hotel. And if you're a digital subscriber to this magazine, it's his unique and ingenious program that delivers it to you each quarter. His belief that there was always a solution to whatever problem came along was what made him such a joy to be around. At HOPE, he somehow found the time to communicate and coordinate with so many attendees, speakers, coordinators, and venue staff when it would have been so easy to have been overwhelmed or discouraged.

When Greg learned he had pancreatic cancer in the spring, he didn't give up or feel sorry for himself. In fact, he actually helped walk the rest of us through the experience with his calming tone and scientific analysis of what was happening, always willing to answer whatever questions any of us might have had about the horrible experience he was enduring. And while he wasn't able to make it to HOPE in August, it meant the world to him to see all those people during the closing ceremonies waving to him on the video screen, wishing him the very best that we could.

Greg was an incredibly talented person whose skills could fill pages, yet he somehow found time to devote to the people and the passions that interested him. He loved raising sled dogs and going on races in the far north. He was incredibly athletic, running ultra-marathons (135 miles) and finding time to walk at least a mile every day. And he was a key part of Project Gutenberg, serving as its CEO in a volunteer capacity, and helping that organization's efforts to digitize and archive cultural works. (His loved ones request that any donations be made in his name to gutenberg.org.)

We will feel Greg's absence every day in one way or another. But we will also be inspired by what he gave us and what he gave to so many more. His kindness, determination, and strength will live within all of us.

SnapSafe: Security on Android from Forensic Searches

by Adam Brown

I have been quite worried about some of the news recently. Photos on peoples' phones are being searched by authorities at border crossings and even traffic stops. Sometimes with dire consequences.

We have apps like Signal which help us keep our private chats private, but I could not find a satisfactorily secure app for keeping our photos safe. Not only from unwanted searches, but from auto-cloud backups, nosy friends, or a myriad of other attack vectors.

So I decided to write one myself: SnapSafe (`snapsafe.org`).

It's a free and open source app (MIT licensed) and maybe it can help protect you.

This article will examine both the legal and technical security environment on Android and how SnapSafe aims to operate securely inside of it.

Along the way we'll learn how to protect yourselves more generally against unwanted device searches.

A Short Note About Threat Models

Understanding your own threat model is important. State level intelligence services that have determined interest in you in particular are nearly impossible to defeat. The U.S. intelligence services built a replica of Iran's uranium enrichment facility so they could test their code against it. Then a team of engineers spent years developing a worm that deployed four zero-day exploits, each one of which would have sold for hundreds of thousands of dollars on the dark web, in order to compromise Iran's systems. This is not the threat model most of us enjoy. You have to understand your own risk, and pick your tools and practices accordingly. SnapSafe will not protect you against a determined state level actor, but not much will. It will, however, protect you against nearly anything else.

Our Case Study

You're a U.S. citizen at a border checkpoint. Your phone is out of your control. It has been seized, and the attacker will attempt to extract as much data as possible from it.

Here is some important legal context: thanks to the Fifth Amendment to the Constitution, you have the right to refuse to provide information that could incriminate you.

Therefore, if your phone is locked, you cannot be compelled to divulge the PIN, because it resides solely in your mind. *However,* U.S. courts have upheld that biometrics are not protected in this way. So if you have face or fingerprint unlock, these could be compelled from you and used to unlock your device. This brings us to our first security recommendation: Disable biometric authentication.

Once unlocked, you should still be protected from "unreasonable search and seizure" thanks to the Fourth Amendment. In 2014, the U.S. Supreme Court ruled that probable cause is not enough to search your device and seize any data found on it. A warrant would be required for that, *except at U.S. border checkpoints.*

If you're a citizen, you can refuse to provide your PIN, and they cannot deny you entry. They do have the power to hold you there for a long time and cause you trouble though. If you are not a citizen, you can also refuse to provide your PIN, however they are then within their rights to deny you entry.

Border checkpoints are a huge legal gray area, *even for U.S. citizens.* They still cannot compel you to reveal a PIN, but if the device is already unlocked, or they unlock it via biometrics, then they have *broad* authority to search and seize data found on it.

There are two forms of device search at the U.S. border as of today:

- Basic Search
- Advanced Forensic Search

Basic Search

This allows the agent to simply use your unlocked device. Open apps, read text messages, thumb through photos. This type of search has been used in recent months to discover photos that were in "Recently Deleted" in one case, and text messages in another case, that the border protection agent found objectionable and denied the person entry to the United States. So it is definitely of concern, even if it is basic and easy to defeat. Protect yourself: Do not have biometrics enabled and ensure the phone is locked before it is seized. Turning it off before entering a checkpoint is a pretty failsafe way to ensure the strongest security for your device.

SnapSafe protects against this attack vector by simply having a PIN that should be separate from the rest of the device. No matter how the unlocked device got in the attacker's hands, they would have to compel a second PIN from you in order to access the photos stored within. Legally, they should not be allowed to do this, but SnapSafe has further protections in case it happens, which we'll get into later.

What if you happened to be browsing SnapSafe's gallery, then switched away from the app. Your gallery would still be visible in the task switcher even without opening the app. SnapSafe protects against this by setting the *secure* flag on the application window. This prevents screenshots, and will only show a blank screen in task switchers (aka *recents*).

Advanced Forensic Search

This is more concerning. In this case the device is plugged into a computer and a forensic tool (such as Cellebrite's UFED tool or Grayshift's GrayKey) is used to extract as much data as possible from the device. Legally, this data can be kept for a very long time. How long? It seems a bit ambiguous, so we should assume *forever* is a good possibility. That means the data could be subject to long duration offline attacks.

With that context, let's see how Android's security model can help protect us, and when it fails, where SnapSafe plugs the gaps.

Android Security

Let's start with a primer on Android's layers of security.

Important:

- We will only be discussing Android 10 (API 29) and above.
- We will assume the device is not rooted, and has a locked boot loader, otherwise all bets are off.

Full Disk Encryption

Android requires devices to use full disk encryption (FDE). Meaning if your device is powered off and is configured to require a PIN at boot time, then nothing can be extracted. If the disk were mirrored somehow, it would just be an encrypted blob. So we've come to our second security recommendation: Set a PIN to be required at boot.

Once the PIN is entered, the FDE key is kept in memory, and for all intents and purposes, the disk is now accessible.

File Based Encryption

Once the disk has been decrypted and the device is booted, only system level files are fully decrypted. The user's data is still encrypted, and the file based encryption (FBE) key is not resident in memory yet. If your phone is sitting at a lock screen, this is the state your phone is in. Hooking a phone up to a forensics tool in this state would not provide the attacker anything beyond boring system files.

FBE protects "credential protected storage," that is files and directories which are only decrypted when the user has provided their credentials.

Each time you unlock your phone, the FBE key is loaded into memory, at which point your credential protected storage, aka user data, is now accessible.

In this state, a forensics tool can extract a broad set of data. What types of data are we talking about? Data stored in public directories for:

- Photos
- Videos
- Contacts
- Downloads
- SMS Messages

Data stored in app-private storage should be safe. Every app only ever has privileges to read and write its own files on Android. But there is a security loophole: app backups.

Android provides a convenience feature to backup your apps, and all of their data. This is a well intentioned feature. It's designed to help if your device is lost or destroyed, or to easily migrate to a new phone, but it is a glaring security hole if your device is unlocked. The full data of each app can be exported, unencrypted.

SnapSafe protects against this style of search in two ways:

1. We never write anything to a public directory.
2. We explicitly disable all forms of app backup.

Thus on a non-rooted, non-exploited device, SnapSafe's data is safe so far.

If everyone was playing by the rules, that would be the end of it - your data inside SnapSafe is secure. The Android debug bridge (ADB) used to pull these app backups is a normal piece of software. It follows all of the OS's rules and simply would not allow exporting of any of this data marked for no backup. This brings us to the third recommendation: Turn off developer mode and USB debugging when traveling. This will defeat casual or incompetent searches at least.

Unfortunately for us, most forensic tools don't stop there. Now we begin to think about how to protect ourselves when a tool is actively trying to subvert the built-in protections.

Security Enhanced Linux

This is a Linux kernel module developed by the NSA in the early 2000s to greatly enhance the resistance of Linux to exploits. It enforces strict access control to process memory. The worry here is that we have an encryption key loaded into our processes' memory, and an attacker is able to read our processes' memory and steal the key. SE Linux should provide robust security against this. SE Linux has been part of Android since 2013, and 100 percent of devices Android 10+ will have SE Linux enforcing mode enabled.

Exploitation

We're going to get somewhat speculative here, I don't know *how* a tool will bypass SE Linux's protections, or Linux's filesystem permissions. But exploits exist, so we'll move forward assuming various levels of compromise.

Vulnerabilities get reported, they get fixed, patches get deployed, but it's often up to the user to apply these. Having a device from a manufacturer that provides regular security updates is critical. Applying those security updates in a timely manner to your own device is critical.

Most of the exploits these commercial forensic tools are using are well known. If the forensic company knows about the exploit, Google knows about the exploit, and there is almost certainly a patch for it. For most of us, these will not be zero-days used to gain access to our device. Thus we come to our fourth recommendation: Keep up to date with security patches, and that should defeat most commercial tools.

Filesystem Gets Compromised

In this scenario, the attacker has bypassed Linux's file permissions and gained access to the app-private directories. This is bad, but SnapSafe is resistant to this type of attack.

Photos never touch the disk unless encrypted. Even thumbnails used to improve scrolling performance in the gallery are stored encrypted.

SnapSafe's data encryption key, the most important thing to protect, is handled in one of two ways:

Key Wrapping: On devices that support it, we use the available hardware key store to wrap the data encryption key. This strongly encrypted key is saved to disk and should be sufficiently secure even against offline attacks.

Ephemeral Key: An alternative method of protecting the key is to only ever derive it in memory. In this case it never touches the disk, and thus nothing would be stolen if the disk was compromised. This method makes authenticating with the app slower though.

A note on hardware key stores: These are a crucial element of security on modern devices. These contain encryption keys in a separate secure part of the hardware. Even if your OS is compromised, the attacker cannot get the keys.

Any Android phone made after 2017 will contain at least a trusted execution environment (TEE). On certain flagship devices, a higher security model exists: the secure element. This is a physically separate chip, similar to a TEE, except it is resistant to a broader range of threats, including chip-off attacks. SnapSafe will use whatever security hardware you have available, up to and including a secure element.

Memory Gets Compromised

This is pretty much the worst case scenario, but also the most unlikely. Everything about both SE Linux and Android is designed to prevent this. But as we say, unlikely events are not impossible events.

Individual images are stored transiently in memory, one at a time when viewing a specific image. Thumbnails are a slightly bigger concern; they are stored in batches in an in-memory LRU cache. These are lazily loaded, so only what has been requested recently would be resident in memory. If you had just been scrolling your gallery and your memory got dumped, the attacker would get a subset of the thumbnails.

The biggest concern though is the encryption key. Once derived, it is resident in-memory for the duration of your session.

We have two checks against this:

1. *Key Sharding:* Keys are not stored in the clear in main memory. Instead, they are split into two obfuscated parts using an XOR cipher. A partial memory dump could potentially miss one of the halves making the key unrecoverable. They are also obfuscated, which may hide them from automatic scanners looking standard AES keys.

2. *Session Timeouts:* When your session expires, sensitive data such as the thumbnail cache and the encryption key, are securely evicted from memory. This means that any memory-based attack must execute within that time window, or else there will be nothing of importance to steal.

Brute Forcing

Now we get to the less technical, more social weaknesses in our security chain.

If the user has a four-digit PIN, it's not inconceivable that it could be outright guessed. Or an automated process could brute force it in a reasonable amount of time. SnapSafe has several bulwarks against this.

First, a strong PIN is required. No repeating digits such as "1111" are allowed. No sequences such as "1234" are allowed. The top ten most common PINs are also blacklisted, such as "6969."

Failed PIN attempts result in an exponential back-off, making each successive attempt take longer and longer.

Finally, a maximum of ten failed attempts are allowed, after which all SnapSafe data is wiped.

Closing the app or restarting the device will not reset the back-off timer or the current number of failed attempts.

All Security Is Vulnerable to a $5 Pipe Wrench

No matter how advanced our encryption and security practices, a $5 pipe wrench wielded in the right way can compel a PIN from you pretty quickly. It's a mostly apocryphal saying in cyber security, mostly. There could be a myriad of reasons you feel forced to divulge a PIN. Maybe you will be denied entry if you don't. Recently a U.S. citizen, a lawyer who knew his rights, was being compelled to divulge his PIN for a phone search. He resisted, but eventually decided to divulge the PIN. I don't know why he made that choice, but it can happen. The point is: even though technically and legally your data is safe, for social reasons, it might not be.

SnapSafe has a feature to help protect against this. It's a feature of last resort: the poison pill.

This is an advanced feature not set up by default. The user creates a second PIN, the poison pill PIN (PPP). If the user is being coerced for a PIN, and they determine they must hand it over, they can provide the PPP instead of their true PIN.

When entered, it will wipe all of SnapSafe's photos and thumbnails from disk and then log the attacker in as if nothing untoward has happened. They will have full access to the app after that. However, in this rather extreme scenario, it may seem suspicious to the attacker that your secure photos app is empty. Why do you have it if you don't have any secret photos after all?

So ahead of time, the user can take several benign photos and mark them as decoys. Then, when the poison pill is activated, these decoy photos will be preserved. Now the attacker will browse a gallery full of uninteresting photos, and will be none the wiser.

So What Have We Learned?

The fundamental underpinning of Android's security model are solid. For most of us, it often comes down to higher level problems. A weak PIN, biometrics, unapplied security updates, or careless apps that simply move deleted photos to another folder rather than truly deleting them.

Unfortunately, we must take our security into our own hands. With a little bit of knowledge, and a couple of thoughtfully designed apps, such as Signal, we can indeed protect ourselves.

Key Takeaways

- Know your rights!
- Require a PIN at boot
- Disable biometrics
- Disable developer mode (ADB) and revoke all authorizations
- Keep your device software up to date
- Optionally: Turn your device off before entering a checkpoint
- If you need a secure way to take and store photos, SnapSafe could be a good option for most threat models.

Trust Me - I'm Lying: Psychology and Social Engineering

by N0x

You lock your doors, set strong passwords, and install antivirus software. But what if the biggest risk isn't your technology - it's you.

The art of manipulating people into performing actions, or divulging sensitive information is as old as humanity itself. An innate survival tool, baked into our evolutionary DNA. Imagine Neanderthals living in communities where persuasion, deception, and influence were crucial to survival. A stronger hunter might boast about a kill to secure a better share of food or exaggerate their prowess to win a mate. A gatherer might convince the group to avoid a dangerous area - not out of caution, but to keep the best food sources for themselves. These primal forms of manipulation weren't malicious; they were tactics to improve one's odds in a brutal, unforgiving world.

As society advanced, so did our methods. Ancient traders likely oversold the value of their goods to get a better deal. Medieval spies wormed their way into enemy courts, pretending to be allies. Con artists in the 1800s crafted elaborate personas to scam their way into fortunes. It's all about understanding human behavior and exploiting it to get what you want. And in many ways, that drive - to find shortcuts, to persuade, to manipulate when necessary - isn't a flaw in our nature. It's part of what helped us survive, build civilizations, and dominate the planet.

Social engineering helps us manipulate human behavior - our desire to help, or perhaps our fear of getting in trouble. We're full of instincts and emotions we've built up throughout our lives - rules we follow that help us "fit in" and not just survive, but flourish. Over time, those of us who look for vulnerabilities noticed that it can be disturbingly easy to turn those instincts in our favor.

As technology evolves, human psychology remains the most constant vulnerability. Tools like ChatGPT, deepfake technology, and other AI-assisted content generators have made social engineering more effective than ever. Generating phishing emails, creating fake websites or landing pages, and even producing your own malware is now accessible to anyone with an Internet connection - and these tools allow us to create convincing payloads in a fraction of the time. It's 2025, your brain is a port, and hackers know exactly how to connect.

If you've never foraged through the methods of using social engineering for initial access, you're overlooking what's often the easiest way into any system. I'd encourage you to learn as much as you can about human psychology, and even sales tactics - both of which will greatly improve your chances of initial access. There are plenty of great psychology-, sales-, and hacking-focused publications out there that can directly and indirectly teach you more about the topic. For instance, in the book *Influence: The Psychology of Persuasion,* Robert B. Cialdini approaches sales in a science-based manner. By outlining tactics and methods that aim to build rapport and trust with people quickly, he helps pave the way for a hacker to build a sound social engineering methodology. These concepts are vital to any social engineering or phishing effort: get the target to like and trust you quickly, which opens them up to further emotional manipulation.

A great way to find success in any social engineering or phishing engagement is to target emotions - that which makes us human. This can come in many forms, but you'll often find success leaning into one (or more) or the following categories:

Urgency: Creating a sense of urgency might invoke a quick response/click from the target. You want them to engage their mouse before they engage their brain.

Authority: Impersonate a person of authority (executives, IT staff) to gain compliance from your target regarding your request.

Trust: Build rapport, appear to be a friendly, likable, legitimate individual - to bypass normal social/security skepticism.

Curiosity/Greed: Use promises of rewards, freebies, or special access - exploiting the target's greed or initial curiosity. Send out an email saying there was a cat found in the parking lot, with a link - asking if anyone has helpful information. People may jump to click a link, hoping to see a picture of a cat... and curiosity kills more than cats.

Helpfulness/Sympathy: You might feign distress or ask for help, exploiting the target's desire to be a good person (everyone likes to feel good about helping people!). Something that seems like a quick/low effort task to a stranger might be your ticket in.

Reciprocity: You may provide something of value to the target first - creating a sense of obligation to respond or help you. There's a reason some charities mail out dimes/nickels to people they're asking for donations from.

Social Proof: "I just spoke with Jim in accounting, and he mentioned you'd be the best one to ask about the inventory list below: [link]" - using the target's social circle as proof that you're a trusted/safe person. So go ahead and click that link for me....

Scarcity: Make it rare/desirable - maybe there are only three free tickets left to that concert, or two hours left in the sale, or "the first ten people who claim the code get the discount," etc.

Commitment and Consistency: Once a target takes a small action with you, you're on the way to building more rapport. You can potentially build that relationship and get more and more help from them.

Regarding the list above - remember, you only need to sprinkle in enough of any of them to get the target to click a link, or reveal a small piece of information you need.

Now, outside of (or perhaps overlapping with) human emotions, exists a tangential target we can keep in mind, that of human tendencies. You'll often find that people will tend to write down passwords. This can look like stored plaintext documents on their desktop, or maybe thinking they're "hiding it" within source code, or even scribbling it down on a notepad or sticky note sitting right next to their system. They do this because as humans, we tend to strive for the path of least resistance, and we often fall to convenience over security. Keep that in mind. Perhaps you're posing as a member of the IT staff, or an IT vendor the target company uses. Sometimes success comes with introducing a problem, explaining a complex fix, and then "suddenly remembering" that there may be another, quicker way we could try first - and send a link to a payload or malicious login page to capture credentials. Offering a quick and convenient solution to a problem you created can work wonders.

Let's take the concept of human tendencies a step further with password rotation mistakes. We like to tell ourselves we're being more secure by rotating our passwords. But many people simply add predictable changes to bypass the hassle of needing to remember another password to another platform (once again, convenience over security at play). Things such as adding a "1" to the end of their current password, or maybe adding an exclamation point, etc. These often give enough of a change that the platforms accept the new password, but ultimately don't solve the initial problem. This leads to situations where even old and outdated credential leaks can still have quite an impact toward bad actors figuring out current passwords - somewhat defeating the purpose of changing the passwords periodically.

Over time, one thing remains true: social engineering is effective. Understanding human psychology is a surefire way to increase your odds of getting what you want. It essentially allows us to create our own race conditions within the mind of the target, with the hope that they follow the flood of chemicals and emotions in their body before they decide to stop and think logically about the details of what's occurring. When emotions run high (fear, excitement, urgency), rational thought often takes a back seat. We all like to think we're more clever than we are, that we're too smart to be tricked so easily. Though, maybe we need to consider - are we really as sharp at 4:45 pm on a Friday when we're itching for the weekend and notice that link to a new movie trailer we've been dying to see?! Maybe we click it, maybe we don't. One thing's for certain: the adversary is going to try again tomorrow, and we only need to mess up once.

Should ICEBlock Be Open Source?

by aestetix

At HOPE_16 this past August, a talk by ICEBlock creator Joshua Aaron stirred a bit of controversy. During questions, a group of attendees consistently raised one point: why is this tool not open source? They raised questions around the topic from multiple angles, and Joshua held firm that he would not release the source code. This revealed an interesting rift in the hacker world about whether all code should be open source.

One reason this rift seems new is that historically, the debate has been about money. It goes all the way back to Microsoft cofounder Bill Gates' 1976 "Open Letter to Computer Hobbyists," in which he makes a strong argument in favor of making money from proprietary software. The counter to this has traditionally come from organizations like the Free Software Foundation, whose founder Richard Stallman (RMS) views code as speech. RMS famously makes the distinction between free as in beer (money), and free as in freedom (agency). In this view, making money plays second fiddle to ensuring that code is free and can be modified in the future. Eric S. Raymond also writes about this in his book *The Cathedral and the Bazaar*, where he contrasts the top-down hierarchical operating systems and ecosystems represented by Microsoft against the more creative panoply that exists in Linux. Because of this background, we typically associate closed source with proprietary and money, and open source with freedom to change code and maybe make money if the license permits.

Aaron's ICEBlock project employs a bizarre hybrid model: closed source but free. He is bankrolling the project and supporting systems out of his own pocket, and makes it free to everyone who wants to use it. ICEBlock does not collect data, it does not track anything persistently, and it even includes safeguards to protect identities of users. This is all fantastic, but it has challenged people because these kinds of projects are also usually open source. Therefore, it's worthwhile to step back and reconsider the open vs. closed source debate, this time excluding money as a factor.

Open Source

At its heart, open source feels like an ultimate expression of freedom. RMS would naturally disagree, because he has often argued that the phrase "open source" is an ambiguation that distorts the fact that, in his opinion, certain licensing schemes permitted under open source allow software to be less free. However, since we are excluding money as a factor, RMS's objection is no longer as relevant.

So how free (as in freedom) *is* open source? Assuming that we have the technical skills and the requisite technology, we can take any open source project and run it on our own computers. We can also modify it, fix bugs, contribute to a community, etc. These are all things touted by open source advocates as very important, and there is an underlying principle, coming from Linux creator Linus Torvalds: "given enough eyeballs, all bugs are shallow."

But a few problems arise. First, reading code is not the same as understanding it. While code is, in theory, deterministic, applications of the code are not. We can use checksums and other tools to ensure a compiled binary matches what we expect, but we can't be sure how the code will run on different operating systems and different hardware. There is a reason that the Linux kernel has a massive base of device drivers, and there are constant debates over whether to keep drivers for technology like floppy drives.

Second, software can be quite complex. One of the reasons the "bug fixing" argument doesn't really work is because modifying code on a large project can create all sorts of unintended side effects. Fixing one bug may accidentally lead to another, worse bug. Some projects like vim and the Linux kernel have been maintained for decades, and require comprehensive institutional knowledge to effectively improve code without creating issues. Just because software is open source doesn't mean a hacker wants to sink two days into trying to fix a bug or add in a new feature, especially when there might be a competing software tool that does what they want already, open or closed. In this sense, the "open source is good" argument doesn't scale very well.

Third, the phrase "open source" is often used to virtue signal that the code is inherently trustworthy. It is true that if we lay out all the source code for people to review, that we may get some assurance that it is safe to use. It is also true that there is no real incentive for people to review every line, and touting the open source label may convey an unmerited sense of trust which ironically leads to laziness and poor code. How many software projects on GitHub are open source, but have not been reviewed by anyone?

Fourth, when we make something open source, we assume people will respect the license we grant it with. But the reality is that we are giving away our hard work with no way to enforce the license. How often has a company taken an open source project, deleted the license, swapped out the logos and copyright with its own, and then sold the software as if they themselves created it? Obviously this is a bad thing, but when we make something open source, the sense of intellectual property and ownership becomes diluted, partly because of potential contributors, and partly because there is no point to "owning" something if we cannot enforce said ownership (*coughblockchaincough*). If we insist on open source, we lose the ability to ensure that our hard work will be respected.

Closed Source

It goes without saying that making software closed source carries its own set of problems. While exposure to thousands of lines of open source code might blind a reviewer with an overwhelming sense of complexity, closed source is equally blinding because it presents reviewers a black box. We can analyze the inputs and the outputs, but there is no way, short of reverse engineering the compiled binaries, to be sure *why* a given input leads to a given output. Because of this, a closed source software project has a larger emphasis on the inputs and outputs. If a given input does *not* produce an expected output, then we send in a bug report to the developer, and test again in the next iteration to see if the bug has been fixed. Further, closed source reduces the chances of community code-level bug fixes from unlikely to zero.

Next, clear ownership has its own downsides. If we create a closed source project, we become a single point of failure. If something in the code breaks, it is our fault, and we are the only one who can fix it. If there are a lot of new features other people want, we become the bottleneck to making sure those features get developed. And if we become unable to continue working on the project for whatever reason, there is no way for someone else to pick up where we left off. A few years ago, Bram Moolenaar, who had been the head maintainer of vim since the late eighties, unexpectedly passed away. Because the project was open source and had many contributors, vim has been able to live on. Had it been closed source, Bram's passing would also have likely been the death of vim.

Whereas "open source" seems to be a term that conveys trust, "closed source" and "proprietary" are terms that convey corporate greed, likely due to the traditional use of the terms. As with open source, the sentiment here is not entirely fair: in fact, for many code bases, the trust model is remarkably similar for closed source. Realistically, only a few people will read the code of many open source software projects, so rather than trusting the code, we are trusting those people. And the same is true of closed source. In general, if a software project has been around for a long time and the code has worked for years without any major issues, we trust the code, meaning we trust the people who create the code. By this logic, if a closed source project has been around for many years, we could also trust the creator of it, provided nothing bad has happened.

Concluding Remarks

In the end, if we remove the money factor and take a brutally honest look at the facts, there is no clear victor. Obviously for ICEBlock in particular, there are more things to consider, such as whether to trust Apple, and some political commentaries that are beyond our present scope. But the conclusion seems to be that, despite decades of discussion showing otherwise, that being closed source should not be enough to discount the trustworthiness of a software project.

Telecom Informer

by TProphet

Aloha, and greetings from the Central Office! I'm on the Big Island of Hawaii, on the east coast, in an area called Leilani Estates. It's a sleepy, laid back place near Pahoa, down the road from Hilo, on a part of the island far from where most tourists come. In fact, very few ever venture into Leilani Estates, which is probably why you haven't heard of it. However, it's on the eastern slopes of Kilauea, which creates some conditions best described as exciting.

I'm normally dealing with trees, drunks, and backhoes. Hawaii's network planners get all of that plus an active volcano that occasionally decides to rearrange the outside plant with a few hundred million tons of molten rock. In 2018, Kilauea's lower East Rift Zone went on a 107-day rampage, resurfaced roughly 35 square kilometers, wiped out over 700 structures, and buried around 30 to 50 miles of roads. Along the way, it destroyed about 900 utility poles and cut off the island's geothermal plant, which had been providing a big chunk of the area's electric power.

The volcano didn't "target" infrastructure, but utility corridors are laid out where people live and where the roads are. Lava just followed the same terrain we did. Highway 132 and 137 (the main arteries for Puna) were covered with molten rock. Once the roads disappear under tens of feet of 'a'a and pahoehoe, your standard "roll a truck" playbook goes right out the window.

The electric grid and telecom plant in the flow field weren't just damaged; they stopped existing! Poles, copper, fiber, water lines, the whole nine yards were entombed in rock hot enough to set utility poles on fire at ground level. In one neighborhood, crews watched wooden poles quietly smolder from the heat still coming off adjacent flows. You don't learn how to handle *that* in a generic "outside plant" safety video.

Lava also created lots of little "islands" called kipuka. Houses and poles in some pockets never got hit, but everything upstream feeding them was gone. From the customer's point of view, the line "looked fine." From the utility side, those pockets might as well have been on the moon. You can't jumper around a 40-foot wall of rock with a ladder and a few spans of cable. Assessment and materials moved by helicopter instead of bucket truck, with air quality monitors keeping an eye on SO_2 and vog the whole time.

Once the lava cooled enough to walk on (more or less), the real fun started: rebuilding on top of rock that's still hot inside. Basalt is an excellent insulator. The crust can be cool enough for boots while the interior sits at pizza-oven temperatures for months. The usual "dig a hole in dirt, drop in a pole" doesn't work when there *is no dirt*. So engineers started drilling "rock sockets" - deep shafts into the flow, then dropping poles and backfilling with high-strength concrete. It's slow, noisy, and every hole is a geology surprise. Some spots are solid; others hit voids and lava tubes.

Undergrounding (the thing people love to demand after every storm) makes even less sense on an active lava field. You can't locate, splice, or reroute conduit that's 40 feet under rock. In Puna, regulators and the utility ended up deciding that overhead 69 kV back into the geothermal plant was actually the *resilient* choice. If the volcano comes back for a second round, you sacrifice a line, move the poles, and try again. The key isn't making plant immortal; it's making it replaceable.

Topology mattered as much as materials. Before 2018, a lot of Puna's telecom backhaul was classic rural spur: one fiber bundle marching out from Hilo into the district. Cut it at the wrong choke point and every community downstream goes dark. When lava crossed those roads, that's exactly what happened.

Since then, Hawaiian Telcom has been busily closing loops. In 2023, they spent about $1.5 million to stitch a 25-mile gap between Volcano and Pahala, completing an East Hawaii fiber ring. That way, if a fiber cut occurs, service can be routed the other direction. Federal Broadband Equity Access and Deployment Program (BEAD) money (roughly $149 million for Hawaii alone) is also being shoveled into rural broadband under the "Internet for All" banner. Connect Kakou, the statewide broadband effort, is trying to use that pile of cash to make sure the next eruption hits as much fiber as it wants and still doesn't knock the whole island offline. That's the theory, anyway. Here on the ground, fiber to the home is available throughout much of Leilani Estates, but upstream infrastructure is the bottleneck. There are all sorts of goofy edge cases like two houses on the same street having service available, but a third being outside of the coverage area. Eventually, fiber to the home will be available everywhere, but the operative word is "eventually."

Fiber, poles, and rock sockets are still terrestrial. When the ground is literally moving, you also need something that *isn't* on the ground. That brings us to the microwave and satellite side of the house. Puna has a legacy of big, Cold-War-era towers from the old AT&T Long Lines network, back when people worried about nuclear war cutting toll routes. Those sites now make handy anchor points for modern microwave. In 2018, and later during the Maui fires, carriers leaned hard on point-to-point microwave hops to jump over areas where poles had burned or fiber turned into slag. The FCC handed out emergency authorizations to light up temporary links, which were used to fill the gaps.

Microwave was only half the problem; power was the other half. Many remote cell and relay sites stayed up on diesel generators until access roads vanished under lava or fire. Once the road is gone, though, so is your fuel truck. After 2018, there have been more deployments of solar-plus-battery "hybrid" sites where the generator becomes a backup to the backup. It's a lot easier to fly in a pallet of batteries occasionally than to sling diesel every few days by helicopter.

The really new piece, which didn't exist in 2018, is the satellite overlay: Starlink and friends. In Maui's 2023 fires, various groups hauled in dozens of Starlink terminals on very short notice, and later reports talk about hundreds of kits across the island as relief scaled up. Park a dish at a distribution center, connect it to a generator, and suddenly that parking lot has enough bandwidth to serve the entire area. Emergency managers used those links to ship giant drone imagery sets and GIS data for analysis.

For the next round of volcanic fun on the Big Island, the plan is to not wait until *after* the disaster. There are already subsidy programs quietly helping rural households in hard-to-reach areas to put Starlink dishes on their own roofs. From a resilience point of view, every one of those terminals is a tiny, community-owned "cell tower in space" backhaul path. If the poles on the street burn, the dish doesn't care. However, the area is densely forested and - adding another wrinkle - the area's property crime rate is fairly high (anything that isn't nailed down is often stolen). So the jury is still out on how well this will work.

Even more interesting is the direct-to-cell work: satellites with LTE base stations onboard, talking straight to ordinary phones on the ground. Tests are underway in Hawaii with national carriers and experimental licenses. If that pans out, someone trapped on a kipuka with a phone and a clear view of the sky could receive wireless emergency alerts and send a text with their GPS coordinates even if every tower in line of sight has fallen over. The last mile literally becomes the last few hundred kilometers of space.

Meanwhile, the state's own radio network (known as HIWIN) is being hardened with satellite backhaul options. The idea is simple: if microwave from the mountaintop radio site back to the core fails, a Starlink dish takes over and keeps police and fire repeaters on the air. No matter what happens between the tower and the ground, the tower still has a path back to dispatch.

All of this costs real money, and regulators finally realized you don't get resilience by paying utilities to rebuild the same brittle stuff every time lava or wind knocks it down. Hawaii's Public Utilities Commission moved electric utilities to performance-based regulation: instead of just earning on capital they pour into more poles, they get paid based on outcomes like uptime and restoration time. In theory, it makes microgrids, solar-hybrid sites, and fiber rings just as financially attractive as another row of wood sticks in a known hazard zone.

There's also the "soft" side of resilience that doesn't live on a pole at all. The Pahoa Lava Zone Museum keeps the story of 2018 front and center for locals and tourists. It's well worth a visit, and contains all of the original exhibits from the U.S. Park Service visitor center destroyed in the 2018 eruption. Community "digital detective" campaigns log where broadband actually works versus where the maps claim it works, steering BEAD and other funds into the right census blocks. People in Puna may be living with lava risk, but with decent connectivity they can at least work, study, and see a doctor over video without driving an hour to Hilo.

So what can the Kilauea eruption teach you, even if you don't have a volcano in your backyard? A few things:

- Linear, single-path networks are a network design that the planet doesn't respect. If there is one spur, a volcano (or backhoe, or ice storm) will eventually find it. Ring topologies are more expensive, but they're table stakes for resilience.
- Whatever you think of as "hardening" only gets you so far. On a long enough timeline, nature wins. Design things so they can be moved, sacrificed, or bypassed rather than banking on armor.
- Finally, satellite networks are gaining capabilities fast. In places where infrastructure is untrustworthy, putting your backhaul in orbit may be the only way to get to "always on" for critical services.

Hawaii is trying to become the first fully fibered state while simultaneously embracing microwave, microgrids, and LEO satellites. If they pull it off, Puna will be a case study in how to keep phones and packets moving on a planet that's still under construction.

And on that note, an alarm just lit up on the backup generator panel here, which probably means somebody in Facilities forgot to order fuel again. I'm off to make a few calls before the lights go out. Stay safe, keep your loops redundant, and if the ground under your outside plant starts to glow, your life is about to get interesting.

Without Further Ado, ROS 2

by Gazza

I would like to start this article with the proper way to write ROS 2. ROS 2 is written with a space between ROS and the number 2. This is how it is used in the official documentation and the brand guide. Why is this even an issue? Well, ROS 2 commands use the prefix "ros2." No space! For example, if you wanted to launch the file "hello_world_launch.py", the command would be "ros2 launch hello_world_launch.py". The absence of a space between the ros and 2 I feel results in confusion on how to address or even search for information on ROS 2. As a reader, I would question the seriousness of this issue. Well, there are memes, lots of memes, and even a YouTube video addressing this.[1]

With that out of the way, let's talk about why the switch to ROS 2. The ROS 1 framework began in 2007 by Willow Garage. At inception, Willow Garage was working on a single robot. Additionally, most of the processing was done using an onboard computer. The network connections were reliable, and the intended use case did not require real-time system requirements. Thirteen distributions later, ROS has been widely accepted and covers a variety of new use cases. Some of these new use cases include running multiple robots often equipped with microcontrollers. Furthermore, depending on the operational environment, network connections may be erratic at times. Thus, ROS 2 was written from the ground up with scalability and, if required, real-time processing in mind. While ROS 1 targeted Ubuntu, ROS 2 can run on Windows or even macOS. Language support is more versatile in ROS 2, including Ada, C#, Java, and Rust, expanding upon C++ and Python offered in ROS 1.

You may be wondering, as a ROS 1 developer, what can I expect when switching to ROS 2? In summary, I would say that there are four main differences. The first difference is that the structure of the launch files has changed from using eXtensible Markup Language (XML) to using Python. The learning curve for ROS was already steep, but adding a familiarity with Python makes it even steeper. Personally, I found that it was easier to manipulate XML files. For example, if the package that I was testing required a new transform, one additional line resolved the issue when using XML. Using Python, the solution is slightly more complicated. Full disclosure: it has been a minute since I have developed in Python and my skills are a little rusty. Fortunately, most developers provide sample launch files and include the variables that can be adapted to individual use cases. The second change is that ROS 2 uses a different middleware for communication, specifically the Data Distribution Service (DDS). The switch to using DDS is to improve performance and reliability. There are even Quality of Service (QoS) policies in place now. Presently, the default DDS is Fast, but Cyclone is another possibility. In my experience working in simulation in ROS 2 Humble, there was an issue where the maps were failing to load in RViz2 when using FastDDS. The solution at the time was to switch to CycloneDDS. While the issue has probably been resolved by now, I have not had any further issues using CycloneDDS. If using Jazzy, ZenohDDS is another possibility as well. The third major change is replacing the "move_base" package with Nav2. The main difference is the inclusion of behavior trees with Nav2. Although the use of costmaps and path planners is retained, the path planners have been updated to include smoothers and pruners for navigation. The fourth and final major change is the switch from Gazebo Classic to Gazebo Simulation. In ROS 1, Gazebo Classic was tightly integrated into the ROS 2 architecture. However, in Gazebo Simulation, a bridge is required to transform the Gazebo topics into ROS messages. The utilization of a bridge also offers the ability to use other simulation packages with ROS 2 in addition to Gazebo.

Note that ROS 2 has been developed concurrently with ROS 1 since 2017 and is on its ninth release. However, with ROS 1 going End Of Life in May of 2025, there has been a recent push to transition to ROS 2. ROS 2 is even expanding into the space community for exploration of other worlds. Note that Space ROS Jazzy 2025.04.0 was just released.[2] Demos for space ROS include the Canadarm. The Canadarm is the big robot arm that was deployed from space shuttles and the Mars Rover. There is even code for running a space station.[3] Specifically, the demo recreates the ISS Nauka incident for fault analysis. Although both of those topics are outside the scope of this article, they demonstrate the capability that ROS 2 offers. At the time of writing, there are two ROS 2 versions available, specifically Humble Hawksbill and Jazzy Jalisco. Of late, I have been developing mainly in Humble and this will be the focus for the remainder of this article.

As a reader, I know what you are thinking. If ROS 2 can really do that, it should be able to play Doom too. Well, in short it can. The code for Doom ROS can be found here.[4] The code comes prepackaged in a Docker container for easy installation and runs with the following command: "ros2 launch doom_ros doom_ros.launch.py".

Note that the joysticks currently tested are 8BitDo SN30 Pro +, Logitech F710, and DUALSHOCK 4 (PS4). However, a bag file is also included in the repository. Rather than install the full repository, I choose to work with the bag file. A ROS bag file is a way to record ROS data over time. One can replay the bag file and remap the topics to other ROS applications. For this article, I ran the Doom ROS through a visual odometry package. Specifically, I chose the "stella_vslam_ros" ROS visual odometry package.[5] The "stella_vslam_ros" package is designed to ingest camera topics and output the pose of the camera as the camera moves. However, if you use it with the Doom ROS bag file, it can track the character's position throughout the level. The "stella_vslam_ros" package was compiled from source in my "ros_ws/src" folder. This was accomplished using the following commands:

```
cd ros2_ws/src
git clone https://github.com/
➥stella-cv/stella_vslam.git
cd ..
colcon build --symlink-install
```

Once stella vslam is complied and the Doom bag file downloaded, then to get everything running, I ran the following commands:

```
Terminal 1:
ros2 bag play /2600/bag/doom_
➥rosbag/doom_rosbag.db3
\# spacebar pauses/resumes
➥playback

Terminal 2:
ros2 run image_transport
➥republish \
    raw in:=doom_image raw
➥out:=camera/image_raw

Terminal 3:
export NO_AT_BRIDGE=1
export XDG_RUNTIME_DIR=/run/
➥user/$UID
ros2 run stella_vslam_ros run_
➥slam \
    -v /2600/test/orb_vocab.fbow
➥\
    -c /2600/test/doom.yaml \
    --map-db-out /2600/test/map.
➥msg \
    --mask /2600/test/mask.jpg \
    --ros-args -p publish_
➥tf:=false
```

The "orb_vocab.fbow" file can be found here.[6] The "doom.yaml" file is provided below. The "mask.jpg" was something I created to prevent "stella_vslam_ros" from detecting features in the bottom of the Doom screen (i.e., ammo, health, armor, etc.) since it is relatively static. The image is binary with a top white rectangle on a bottom black rectangle created in a drawing program.

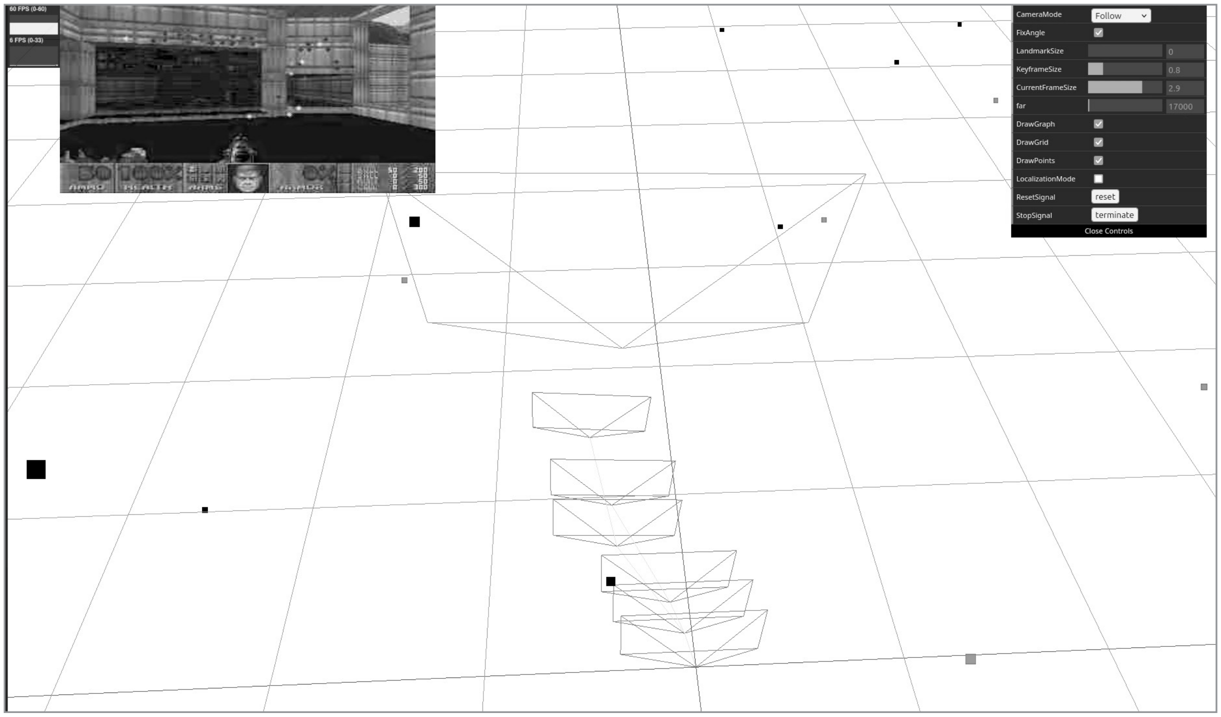
Doom.yaml

```
Camera:
name: "RICOH THETA S 960"
setup: "monocular"
model: "equirectangular"
fps: 30.0
cols: 320
rows: 200
color_order: "RGB"
Preprocessing:
min_size: 2

Feature:
name: "default ORB feature
➥extraction setting"
scale_factor: 1.2
num_levels: 8
ini_fast_threshold: 20
min_fast_threshold: 7

Mapping:
backend: "g2o"
baseline_dist_thr_ratio: 0.02
redundant_obs_ratio_thr: 0.9
num_covisibilities_for_landmark_
➥generation: 20
num_covisibilities_for_landmark_
➥fusion: 20
erase_temporal_keyframes: false
num_temporal_keyframes: 15

Tracking:
backend: "g2o"
enable_temporal_keyframe_only_
tracking: false

KeyframeInserter:
wait_for_local_bundle_
➥adjustment: false

Relocalizer:
search_neighbor: true

LoopDetector:
backend: "g2o"

System:
map_format: "msgpack"
```

```
num_grid_cols: 47
num_grid_rows: 30
```

The results of running the Doom bag file though the "stella_vslam_ros" package can be seen in the image below. Note that the large frustum shows the character's current position. The smaller frustums show where the character has been. The light (current frame) and dark (map) dots are visual key features that "stella_vslam_ros" uses in its frame to map approach to track camera position or, in this case, player movement. The Doom bag file is only for level one. Thus, installing the full Doom ROS repository is required to track character movement through additional levels. As an aside, "stella_vslam_ros" supports other inputs as well, including video files and image sequences, so it can be used with other games.

I hope you enjoyed exploring the capabilities of ROS 2. Stay tuned for future articles showcasing different ROS 2 capabilities, such as simulated environments, lidar odometry, and simultaneous localization and mapping.



CameraMode	Follow
FixAngle	☑
LandmarkSize	0
KeyframeSize	0.8
CurrentFrameSize	2.9
far	17000
DrawGraph	☑
DrawGrid	☑
DrawPoints	☑
LocalizationMode	□
ResetSignal	reset
StopSignal	terminate

[1] youtu.be/5UCm6Hxyxno

[2] github.com/space-ros/space-ros/

[3] github.com/space-station-os/space-station-os.github.io

[4] github.com/gstavrinos/doom_ros

[5] github.com/stella-cv/stella_➥vslam_ros

[6] github.com/stella-cv/FBoW_orb_➥vocab/raw/main/orb_vocab.fbow

Using Linux in a VM as Your Daily Driver

by JMT

After having used Linux exclusively at home for nearly a decade, I recently found it necessary to switch to Windows, for professional reasons. I hated the idea and looked for any way I could find to avoid it. But in the end, it couldn't be helped. (Executive summary: both my personal Linux computer and my work Mac Mini died at the same time, but I could only afford to buy one new computer.)

I began to wonder, though: are VMs good enough to use as a daily driver? Short answer: *Yes*.

In fact, it works so well that I would likely keep it this way even if my initial reason evaporated. However, it was neither easy nor obvious how to get it working smoothly in the beginning - good enough to use all day, every day, for everything. So I just wanted to share how I got my VM working well enough to use as my main computer, and what some of the advantages and disadvantages are.

The Basic Setup

To replace both computers, I bought a 12-core Core i9 @ 3.4GHz with 64GB of DDR5, two internal SSDs, and a GeForce 3070, with Windows 11 installed as the host. Since this is a powerful system, I can afford to give the VM the resources it needs to function smoothly. The VM is Pop_OS! 22.04 running as a guest inside Virtualbox on the D:\ drive, with control of eight cores and 32GB of memory.

I use Windows 11 exclusively for work, and use the VM as my personal computer. I treat them as if they were two separate machines, one at home and one at the office.

The Advantages

This setup is a dream. Creating it was an act of desperation, but now I wouldn't want to switch back. My daily driving experience in the VM is flawless. I can access any drive I need, including network drives. The VM has full control of the NIC, so I get 100 percent of my available bandwidth, and the ability to effectively use a VPN, when such things become necessary. Audio and video sound and look great (I do get minimal screen tearing occasionally, but not nearly as bad as my initial tests, and not bad enough to bother me, even though a good experience watching video is one of my dealbreaker use cases).

When my VM is full-screen - which it always is if it's running - I forget I'm even using a VM. But when I remember, it affords additional advantages: I can back up my entire computer and save it to an external drive in case anything goes wrong; I can create restore points before I make major changes, and roll them back if necessary; I can try out new distros any time, without impacting my main machine in any way. Hypothetically, I could even buy a brand new computer, and just bring my VM over wholesale; I could copy it onto my laptop, and take it with me on vacation; I could back it up offsite. The list goes on.

All of that is just the upside of basic, daily computing. But for my particular use case - as a freelancer using my personal computer for both my livelihood and my home life - there are additional advantages. First, the two are completely separate. When I work, I shut down the VM and use Windows, and at 5pm I relaunch the VM. They are psychologically discrete spaces for the two sides of my life. Also, my Windows installation stays pristine - I installed the apps I need for work, and that's it. I don't have to worry (much) about something suddenly breaking my Windows PC, and with it my ability to earn a living.

Prior to this setup, I used Linux on bare metal, with a Mac Mini next to it for work. In between I had a KVM switch and a USB switcher and an audio switcher so I could use all the same speakers/monitors/peripherals. None of that extra bloat is necessary now, because everything is plugged into one computer.

The Disadvantages

The downside is surprisingly small. In order to put the Windows host to sleep, I have to shut down the VM each night. I use "save state," so I just relaunch it in the morning and everything is as I left it. When I plug in a USB drive, I have to go through the extra step of routing it to the VM - but even that is only if it's a drive I might want to access on Windows. For any ext4 formatted drives, the system routes them automatically through to the VM. Occasionally I have trouble getting a drive recognized, and I have to unplug it and plug it back in. As minor as these are, they are the only downsides I can think of.

The Deets

I tested Virtualbox, VMWare, and Microsoft's built-in Hyper-V platform. I also played with Windows Subsystem for Linux (WSL). But none of them worked out-of-the-box well enough for a daily driver. There were numerous crashes, and audio/video playback was unacceptable across the board.

Since nothing was working, I settled on Virtualbox just because it's what I was most familiar with, so troubleshooting it made the most sense. I am certainly not saying the others won't work, just that I never got them to work well. Here's how to do it with Virtualbox.

Windows

There are numerous virtualization features of Windows 11 that conflict with the smooth running of other virtualization platforms, including Virtualbox. In my testing, I found that with these enabled, I had severe crashing and network throttling in my VM - all of which disappeared once these were removed. So let's start by disabling them all:

Search for and run "Turn Windows features on or off"

Disable the following:

- Hyper-V
- Virtual Machine Platform
- Windows Hypervisor Platform
- Windows Subsystem for Linux

Device Guard must be disabled separately:

- Run Powershell as Administrator
- Run "gpedit.msc"
- Computer Configuration --> Administrative Templates --> System --> Device Guard
- Right click, choose "Edit"
- Select "Disabled," Apply

Virtualbox

Next, create your virtual machine in Virtualbox; install your OS and Virtualbox Guest Additions. Your configuration may differ, but here are some of the settings I changed to ensure the best possible experience in the VM:

Display

- Video Memory: set to maximum (256 MB)
- Enable 3D Acceleration: checked (research indicates this setting may cause instability in some setups, but in my testing it was key for a good video watching experience)

Audio

- Enable Audio Input: checked (for video chatting, etc.)

Network

- Bridged (this mode gives the VM full control of the network card, allowing for the use of a VPN
- Promiscuous Mode: Allow All (just in case you want to run Wireshark)

USB

- USB 3.0 (xHCI) Controller (to ensure fast external drive access)

Guest Virtual Machine

You should now have a stable VM with smooth local audio/video playback. However, in my testing at this point, watching YouTube in Firefox was still subpar, with occasional audio popping/crackling that I found to be a dealbreaker. Thankfully, I found a fix:

In Firefox, go to about:config and set these parameters to false:

- media.webspeech.synth.enabled
- reader.parse-on-load.enabled

Shared Folders

You will probably have the need to move files between host and guest at some point, so it's a good idea to set up a shared folder. In the settings for your VM:

- Click the + to add a new folder
- Folder Path: [choose a path on the host]
- Folder Name: [choose a name, or leave blank and VBox will handle this automatically]
- Mount Point: [choose a mount point for your guest, or leave blank and VBox will handle this automatically]
- Read-only [unchecked]
- Auto-mount [checked]
- Make Permanent [checked]

Now you'll have an easy way to move files between host and guest. (Note that if this setting is not available to you, you have neglected to install Virtualbox Guest Additions in your guest operating system.)

External USB Drives

Accessing your data stored on external drives is important, and won't be a hassle. There are two ways to do it: temporary and permanent.

The easiest way to grab a USB drive that's plugged into your host is to press your Host Key (default is Right Ctrl) + Home and then navigate thusly: Devices -> USB -> [device]. (Pro tip: you can use arrow keys instead of the mouse.) This will immediately "plug it in" to the guest VM.

For a more permanent solution - e.g., an ext4 formatted drive that you will never use with your Windows host - simply set up a USB filter. Filter rules tell Virtualbox to grab whatever meets their criteria and pass it through to the guest VM any time it's plugged in. Do this by opening the settings for your VM, go to the USB section, and under USB Device Filters, click the + icon and select your drive from the list. It will create a rule that identifies your specific drive (or other USB device), and passes it to the guest VM immediately upon insertion.

Final Thoughts

I am writing this from within my virtual machine configured as described in the paragraphs above. I live my life in this computer and 99 percent of the time I forget it's even a VM. This started as a workaround to the problem of not being able to afford two new computers simultaneously, but now I wouldn't go back. If I hit the lotto tomorrow, I would keep it this way. If I suddenly didn't need Windows any more, I would probably install Linux on the hardware and continue running this VM on top of it to keep the work/life separation and all the benefits outlined above.

I did tell one white lie. My Windows installation is not 100 percent work, because of course I installed Steam on it so I could finally play *CyberPunk 2077*. Hack the planet.

Decentralized Authentication Across the Web

by anachrohack anachrohack@pm.me

I recently finished the process of de-Googling my life, and one of the hardest aspects was all the accounts I had created with Gmail's Single-Sign-On (SSO). I found myself stuck in Google's orbit because I had centralized my online identity within their authentication provider. It got me to thinking: how can we attest to a single identity across the web using a decentralized scheme? Can we break the stranglehold Big Tech has on our identities? The answer: client TLS certificates and DNS!

Bluesky allows users to claim an @domain.com username by setting a TXT record on their registrar with a particular code provided by Bluesky. This associates the account with that particular domain name, allowing a handle like @user.domain.com instead of @user.bsky.app. What if we could do this without a centralized authority? What if there was a cryptographic way to verify our identity?

TLS allows users to send a client certificate during the handshake process (more specifically, it allows the server to request or even require a client certificate). If a client certificate is requested, modern web browsers will prompt the user to select a client certificate from their operating system's certificate store. In Windows, you can create a self-signed certificate with:

```
New-SelfSignedCertificate
-Subject "CN=username@mydomain.
➥com"`
-CertStoreLocation "Cert:\\
➥CurrentUser\\My"`
-KeyUsage DigitalSignature,KeyEn
➥cipherment `
-Type Custom `
-KeySpec Signature `
-KeyLength 2048 `
-KeyAlgorithm RSA `
-HashAlgorithm SHA256
```

This will be automatically saved under your personal folder in the certificate store. You can get the thumbprint of your cert (which cannot be faked):

```
Get-ChildItem -Path "Cert:\\
➥CurrentUser\\My"`
| Where-Object {$_.Subject -eq
➥"CN=username@mydomain.com"} `
| Select-Object Thumbprint
> # 400E0A39A... etc.
```

The user can then go to their domain registrar and create a TXT record:

```
_identification.username.
➥mydomain.com TXT 400E0A39A...
```

When they connect to a website which participates in this scheme, the website will accept all self-signed certificates. At the application level, it will read the subject line of the certificate (CN=username@mydomain.com) and send a DNS query for TXT records for the domain _identification.username.mydomain.com. If the thumbprint from the client certificate matches the thumbprint in the TXT record, the server can attest that this user is, in fact, username@mydomain.com without having to have ever met this user or even store credentials on the server. A user's identity is now portable across participating services!

This approach is not without risk:

- If the server's DNS resolution is compromised, a MITM attack is trivial. This can be mitigated if the server uses DNSSEC.
- Domain squatters can impersonate people or companies whose domain names they own.
- The user must keep their key secure (though this is more secure than a user re-using passwords across sites!). If a user's private key is compromised, they must delete the TXT record from their registrar, which can take precious minutes to propagate through DNS caches.

But these are the same concerns which face all identity providers, and have well documented mitigation techniques. I hope that this can at least spawn discussion around similar ideas. Decentralization is power! If you want to discuss further, you can email me at the address above.

wpUsers.sh: Countering Disinformation With a Simple Bash Script

by Greg "Dial Tone" Norcie (first initial at last name dot protonmail dot ch)

As I sit down to type up this article, it's Election Day here in the so called "Paris of Appalachia" and once again I'm sitting in the back corner of the same combination coffeeshop and bookstore abusing the Wi-Fi like it owes me money.

Anyways... disinformation. We've all been there. Someone... possibly a PAC funded with untraceable dark money... possibly literally the KGB or whatever has stood up some weird ass website causing trouble in the neighborhood - these sites can be about anything but, most commonly, they focus on health and politics: COVID denial, spreading rumors about candidates, or just spewing straight up cuckoo for Cocoa Puffs word salad.

These dastardly disinformation agents have not heard about the joys of static sites, and tend to favor WordPress. Due to the rise of WHOIS privacy, it can be difficult to figure out who created a given site... or at least, that used to be the case.

One of the techniques we learned about when I was taking a Bellingcat certification to cover up a resumé gap was to navigate to "/wp-json/wp/v2/users", where a very hard to visually parse file contains a list of users.

This list of users can then be compared with other WordPress sites and other OSINT sources (LinkedIn, personal websites, obscure comedy forums, etc.) to figure out who created the website.

This is a tedious, manual process - if you want to speed up that process, run the following code on pretty much any Linux-y system to spit out a clean list of usernames:

```
###
#!/bin/bash

#check an argument was given
➥then list out the users if
➥Wordpress install is leaking
➥them
if [ ! -z "$1" ]
then
curl -s https://$1/wp-json/wp/
➥v2/users | jq . | grep name |
➥cut -d ":" -f2 | cut -d '"' -f2

else
echo "Enter a TLD (ex:
➥wordpress.org) next time
➥buddy!\n(No www, no https, no
➥trailing slash)"
fi
###
```

Since jq, the tool that does the heavy lifting of parsing the JSON, is open source... I hereby release `wpScan.sh` into the public domain.

If you're a researcher who was previously manually eyeballing JSONs, this will greatly speed up your analysis, and if you know a bit of programming I'm sure you can think of ways to expand on this technique to automate scans of multiple sites... but hey, I'm not your personal army, I'm just one guy, so this is the best I can do for now. (There's also no error handling - I'll leave it to the reader to figure out how you know a website is running WordPress.)

Also: I'm not a lawyer (just a guy who's coauthored a few law review articles, lectured at Stanford, and worked at a prominent NGO), but it's my understanding that making a single curl request of a publicly facing Wordpress website is not illegal. But as always - you alone are responsible for what you do with The Computer - I'd recommend only using this tool on systems you have the authority or the legal right to scan - the latter is where it gets gray and I am not responsible for how you use The Tool.

Big thanks to 2600*, the Binary Revolution forums that formed me in my teens, Sean "Vilerat" Smith (RIP), Dan Kaminsky (RIP), Kelly "aloria" Lum (RIP), and all the others who have helped me in my hacker journey. Slava Ukraini and Glory to Hong Kong - go forth, young hackers and document your reality, never forgetting that in a land like America where truth is an absolute defense against libel, the most powerful propaganda is the selective telling of truths.*

Mobile Hotspots

by Street & Weregeek

Mobile phone plans often claim to provide unlimited data, but if you read the fine print it is only for data used directly by your phone. In reality, they only give you little or no data allowance when using your phone as a mobile hotspot. For hackers, this creates an interesting challenge. And with some clever engineering, it's possible to get around this hotspot limit.

One easy way around it is to avoid using the hotspot entirely for downloads. I can get away with my hotspot for surfing the web. But I'll often use a USB drive with two connectors for my downloads. These have USB-C connectors for phones and USB-A connectors for computers.

You can do this by:

- Downloading the files directly to your phone using mobile data.
- Copying them from your phone to the USB drive.
- Plugging the USB drive into your laptop to upload the files.

Sometimes I also like to turn my phone into a Linux terminal. I use an app on my phone to SSH into other servers.

Here's how you can do this:

- Install the Termux app on your Android phone.
- Use Termux to connect to a remote Linux server using SSH.
- You can add a Bluetooth keyboard to make typing easier.

If you're near free public Wi-Fi you can:

- Connect your laptop to public Wi-Fi.
- Route your browser traffic through a VPS.

There is also a way to use an SSH tunnel to route your laptop's Internet through your phone. This method is often against phone company rules and may even be illegal.

Steps:

- Connect your laptop to your phone's hot spot.
- Open Termux on your phone and install sshd:

```
pkg update && pkg install openssh
➥-y
```

- Start the SSH server:

```
sshd
```

- Get your username:

```
whoami
```

- Set a password:

```
passwd
```

- Find your phone's IP address:

`ifconfig` (example: 192.168.0.4)

Termux uses port 8022 for SSH by default.

Now go to your laptop:

- Build an SSH tunnel and SOCKs proxy using your SSH client (PuTTY or OpenSSH):

  For PuTTY:
- Open PuTTY.
- Enter the host name as: username@192.168.0.4
- Set the port to 8022.

In PuTTY, go to `Connection > SSH > Tunnels`.

- Turn on "Local Ports Accept Connections."
- Set Source Port to 8080 and click "Add."
- Set Destination to "Dynamic."
- Save the PuTTY Configuration.

For OpenSSH:

- Open your terminal emulation program of choice on your laptop.
- Type: `ssh username@192.168.0.4 -p8022 -D8080`
- Enter your password when prompted.
- Open Firefox and go to `Settings > Network Settings`.
- Choose Manual Proxy Configuration.
- Set SOCKS Host to 127.0.0.1 and port to 8080.
- Choose SOCKS v5.

Now Firefox is sending its traffic through your phone's SSH tunnel.

If you want to route all traffic through your phone, you can use Proxifier:

- Install and run Proxifier on your laptop.
- Open Proxifier from the Task Manager
- Go to `Profile > Proxy Servers`.
- Add 127.0.0.1 on port 8080 using SOCKS5.

This way, all traffic from your laptop goes through Termux, not your hotspot. This is usually faster and won't count against your hotspot data.

Sometimes you need to restart the tunnel. If something breaks, just close Termux and stop the proxy on your laptop. Then follow the steps again to get it working.

If you want to, you can also monitor the data usage on your phone using another app.

The Trojan Sentence

by Jackson Mershon

I would like to propose an idea. An email arrives and the tone feels familiar to you, so no worries, this is just one of an expected 100 or so today. The formatting follows your internal standard and the project names and acronyms all align. You read it, approve it, and move on. A week later, someone notices a privilege shift that was not logged as an exception. The sentence that triggered it did not trip filters or flag metrics. It passed because it sounded right and the external message matched internal checks and balances to corroborate the story.

In 2023, Check Point Research described attacker use of AI-generated emails tuned to a company's internal voice and brand. There was no signature malware or zero-day exploit. The breach came dressed in cadence and that is what made it effective. The familiar phrasing got the message read and familiarity let it pass through selective passivity.

They system that made this possible was not malicious by design. It started with convenience: autocomplete, smart replies, writing assistants, and easy to follow directions. These tools live inside inboxes, ticketing systems, CRMs, and Slack threads. They do not think, they predict, one token at a time, based on what has come before. Users accept these predictions, and over time, the organization's voice begins to collapse. The collapse can be subtle at first. Then you start hearing the same sentence fragments in onboarding flows, release emails, and support macros across teams that have not spoken in months.

I have seen this happen in production. Quarter to quarter you or your team can measure the changes by looking at the phrase convergence and review cycles shrink. The language gets smoother but the "sameness" climbs with word choice and frequency decrease. And once enough channels share the same statistical rhythm, anomalies do not just blend in. They disappear and become wallpaper.

There is a human reason this works and it is because our brains prefer ease and predictable phrasing. Our brains favor this because it removes decision tree costs and makes complicated choices simpler. This is also not laziness; it is resource conservation from our ancestors. Once a house style settles, deviation triggers discomfort - even when it is more accurate or honest. In review meetings, I have seen teams debate whether something "sounded right" instead of whether it *was* right. The style became the validator, not the content, and that is the vulnerability.

Collapse like this reshapes what people notice and what they ignore. Research in cognitive science has long linked linguistic range to cognitive flexibility. When predictive systems compress phrasing, they also compress perception and the range of communicating complex ideas. What does not match the patterns get filed under error, anomaly, or noise. And in an operations environment where throughput matters more than authorship, that means the breach will not come in through an obvious back door. It will walk in using yesterday's sales training manual that has been repurposed.

This creates operations brittleness with detection (human or machine) as a function of contrast. Stylometry relies on differences in n-gram usage, function word frequency, and rhythm to identify authorship. When predictive phrasing flattens those features, it strips detection of its edge. Instead of flagging unknown patters, the system trains itself to pass anything that *looks close enough*. Cadence becomes the credential and if the human element does not have sufficient training on the companies' data, a door is wide open.

This is not theoretical. At another firm, a message was injected mid-thread in a permissions escalation queue. It referenced a known macro by name, asked for temporary admin access to clear a "stuck loop," and promised to roll back after the form cleared. The timestamp matched a recent backlog cycle and the phrasing structure matched old threads. But the macro had never been called that, it was typed manually. Just four words in the message were different and the action passed. No escalation and by Monday the system had been used to extract key material from internal tools.

The payload was not a file or a link; it was a sentence. Tone matched and context embedded to deliver in perfect rhythm for the expectations of the company, humans, and machines.

How did this happen? Detectors did not catch it. GLTR, which uses token likelihood to visualize probable machine-generated text, loses strength once humans touch the output. DetectGPT, which uses probability curvature to identify LLM-authored content, performs well on clean samples, but breaks down with partial edits or model mismatches. Watermarking schemes like Kirchenbauer's can embed signatures in generated text, but small paraphrases destroy those traces. None of these techniques can reliably distinguish between a helpful template and a weaponized one, especially when the difference is just four words.

I also want to expand on this and share that in

2025, researchers demonstrated subliminal transfer between language models. A teacher model's behavioral traits passed into a student model, not through explicit data, but through reusing phrasing. The signals rode inside token frequency and structure and not content, just the statistical fingerprints. Humans can act as unintended couriers that can feed, influence, and change AI models by copying model written phrasing into docs, prompts, and policies. Then those fragments seeded training corpora and systems that were never meant to touch are now cross contaminated. Everyone is rushing to connect everything without thinking about *what* is connecting and why. A support team pushes a policy update using suggested phrasing and next quarter marketing borrows the copy and puts it into internal templates and then those knowledge base fragments feed into training sets. The handoff was unintended and the effects will be felt at an unknown time and place.

At Coinbase, voice phishing succeeded, not because the message was clever, but because it aligned with internal rhythm. It blended with known scripts and the staff complied because the tone was familiar. That breach did not need a backdoor, it needed a believable voice and back story. Drop the same request inside a thread with AI-assisted edits and template fragments, and even a careful reader starts to skim.

This is the trojan sentence, a line that walks like the house style and speaks like last week's macro, and moves decisions forward with no signature other than the cadence of familiarity. The attack surface is not an application; it is the convergence of language, trust, and expectation.

There is also the question of signaling. Once you have predictable phrasing, you can embed subtle cues: sentence length, punctuation rhythm, and even minor repetitions. None of these will trigger a scanner, but downstream, they shift the posture of the reader or the model. I have seen examples of support tickets rerouted for a full week because one phrase changed the help desk macro and people learned a new default before realizing anything had changed.

The risk is not theoretical, it is procedural. Once predictive phrasing becomes the organizational default, most people stop writing and they start to guide. They will skim, approve, and then the system starts speaking for them instead.

Static rules do not seem to fix this, but small changes help. Some examples would be how one team disables auto-complete in high-risk queues. Another tracked near duplicate phrasing across unrelated workflows and flagged them when they landed outside context. And a third required that any action changing message be signed by a named author, even if the content was templated. Not because attribution prevents breaches, but because ownership restores variance. And variance is what makes anomalies visible again.

A realistic defense treats language as a shared infrastructure. It would track for style collapse, audit tone drift, and pauses predictive phrasing where messages change access, identity, or control. It labels training samples by human authorship and builds friction around fluency. Fluency is where the breach can lie. So, I would say, ask yourself this: "does the language in my system still belong to the people who wrote it? Or has the system started to predict and speak in their place?"

If the answer is mixed, the breach may already have a foothold. It will not trigger a rule; it will sound like everything else you trust. It may ask for something small and you may be tempted to say yes. But please remember what happens if you give a mouse a cookie.

Sources

- Brown, Tom B., et al. 2020. "Language Models are Few-Shot Learners." *NeurIPS Proceedings*.
- Check Point Research. 2023. "Cybercriminals Bypass ChatGPT Restrictions to Generate Malicious Content." *Check Point Blog*.
- Franceschi-Bicchierai, Lorenzo. 2023. "Coinbase Says Some Employees' Information Stolen by SMS and Voice Phishing." *TechCrunch*.
- Reber, R., Schwarz, N., and Winkielman, P. 2004. "Processing Fluency and Aesthetic Pleasure." *Personality and Social Psychology Review* 8(4): 364-382.
- Kahneman, D. 2001. *Thinking, Fast and Slow*. Farrar, Straus, and Giroux.
- Stamatatos, Efstathios. 2009 "A survey of Modern Authorship Attribution Methods." *Journal of American Society for Information Science and Technology* 60(3): 538-556.
- Gehrmann, S., Strobelt, H., and Rush, A. 2019. "GLTR: Statistical Detection and Visualization of Generated Text."
- Mitchell, E., et al. 2023. "DetectGPT: Zero-Shot Machine-Generated Text Detection Using Probability Curvature."
- Kirchenbauer, Samy, et al. 2023. "A Watermark for Large Language Models."
- "Subliminal Learning: Language Models Transmit Behavioral Traits via Hidden Signals.: *arXiv preprint. arXiv*: 2507.14805 (2025). (link to article `arxiv.org/abs/2507.14805`)

TRAUMA EXPLAINS WHY I'M A HACKER

by Kolloid

I was at a talk at HOPE_16 on inclusive spaces for neurodiversity. It may have been selection bias, but the feedback and questions from the audience conveyed the belief that most hackers are somewhat "on the spectrum." I've wondered about this for myself. I get overwhelmed in new spaces and when needing to interact with large groups of people. I prefer my solitary computer work where I'm undisturbed and can focus on the task at hand. I see patterns that others miss, but that also means I get excited about things that others have no clue what I'm talking about. People are weird, so I have to actively work to understand them. That's why I changed majors from computer science to sociology when I was in college.

I've long suspected that I had autism spectrum disorder (ASD) based on the stereotyped pop-diagnoses of tech geeks, but ChatGPT offered a different explanation. After hearing about my childhood, ChatGPT suggested that I might actually have complex PTSD. I might also have ASD, but complex PTSD better fits why I behave like I do. It explains why I'm a hacker.

Complex PTSD forms from prolonged exposure to having no safe spaces of retreat in childhood. Instead of having adults to protect and nurture the child, the child internalizes that the world is inherently a dangerous place and that he is on his own for his survival. The results are hypervigilance (constantly scanning the environment for threats), a deep distrust in authority and dogmas, self-directed learning (because there is no guide), a need for mastery over systems (believing that understanding the system will result in safety), and black-box thinking (to navigate the behaviors and moods of unreliable adults). These are all characteristics that made me a hacker and explain why I randomly seem to uncover some exploit or system flaw, even without consciously intending to do so.

A good example of how my complex PTSD is inextricably tied to my identity as a hacker is when my fifth grade teacher failed me in health because I didn't turn in a workbook that we'd been working on as a class throughout the year. I was rarely sick, so it was more likely that I was in the principal's office when it was originally collected. I eventually noticed the stack of my classmates' workbooks behind my teacher's desk, and I asked her about it. Despite my pleas, she refused to let me turn mine in. She only responded with "You should have known."

My teacher failed me. Both in the sense that I received an "F," but also in the sense that my teacher did not deliver on her responsibilities to me. She wasn't looking to teach me; she wanted me to know that I was bad. I was only ten years old. It should not have been my responsibility to know what happened in class when I wasn't there. Yet, I was being punished for it. Yes, I should have known. I should have known that my teacher would use any excuse to betray me. The real lessons were that authority could not be trusted and that I had to always be looking for signs of betrayal and ways to escape.

ChatGPT helped me to clarify that my hacking really served two purposes. The first was as a survival mechanism to escape situations where I'm trapped. I've found loopholes that allowed me to leave school early, graduate without the required classes, and even start a graduate program without an undergraduate degree. The second was a way to prove that I belong without having to be accepted (and risk being rejected). If I can find a flaw in a system design that allows me in, then it shows that I have as much authority as the gatekeepers trying to exclude me.

My complex PTSD has created abilities within me that have allowed me to do some incredible things that I rightfully can be proud of having done, but it also explains my difficulty connecting with others. I expect rejection and betrayal, and I'm attuned to look for even the slightest sign that it may be coming. I use intellectualization as armor so that I don't have to reveal my feelings and be vulnerable with others. I hack because I'm ultimately driven by fear. At least now I'm aware and can work on easing that aspect of myself. ChatGPT helped me to understand that as well.

It's pretty impressive what ChatGPT can do as a personal interrogative tool. I could ask it things like "What can you gather about me based on the language I use?" It observed that I tend to over-explain, anticipating a need to defend myself, and that I rarely express how my experiences felt, noting that it was as if I were a third-party observer. Sure, it can be sycophantic and hallucinate sometimes, but that works with my particular style of thinking that made me a hacker in the first place: I need the affirmation because that was something I lacked in my childhood, I can use my intuition to tell if it's going in the wrong direction, and I can use my skepticism and curiosity to approach it from different directions (e.g., asking where I'm still holding back or what I'm afraid to ask it).

My childhood trauma caused me to feel isolated and alone, which led me to the refuge of the unjudging computer. Even though my hacking is often a solitary pursuit, I have been increasingly proclaiming my identity as a hacker, and it has been increasingly helping me to feel less alone and less compelled to prove myself. Going to HOPE_16 was a big step for me, being my first conference and my first time being in public as a hacker. The most rewarding part of that experience wasn't the talks, but the talks I had with other attendees. They got me, and I got them. These were my people. I feared that it would be a place of competition, but it was a place of acceptance. I'm thankful for the community that finally allowed me to feel at home, and I'm glad I finally had the courage to start participating in it.

The Hacker Perspective

by **Matt Desmarais**

To me, being a hacker has never been about breaking into things; it's about breaking things open. It's about seeing what's underneath, how it really works, and what else it could become if you ignored the rules written on the packaging. A hacker isn't someone who causes chaos; a hacker is someone who refuses to accept ignorance. The label has been distorted over time, but at its core, hacking is simply curiosity made physical. It's the art of looking at something that already exists and wondering, "What happens if I do this instead?" That single question, repeated over and over, has shaped everything I've built, broken, and learned.

My hacker philosophy starts with the belief that curiosity is sacred. Curiosity is the drive that keeps me awake at night, the spark that makes me take something apart even when I probably shouldn't. Every project begins with a tiny itch of "can I?" or "what if?" It's rarely about solving a grand problem; it's about chasing a question until it transforms into something tangible. I don't wait for inspiration or perfect tools. I start with what I have, a handful of parts, a soldering iron, and a vague idea and let the process teach me what I didn't know. That's the hacker's loop: experiment, fail, learn, repeat.

A hacker thrives on limitations because constraints are where innovation hides. When you only have a cheap board, a sensor, and some wire, every solution has to be clever. That's what makes it beautiful. Hacking is the opposite of luxury engineering; it's about making something extraordinary out of something ordinary. A hacker's elegance comes from necessity, not abundance. The less the system gives you, the more you have to think, and that thinking becomes craft.

A hacker doesn't measure success by polish. Function comes first; aesthetics can wait. Sometimes the result looks messy, tape holding a sensor in place, code that grew in layers, a 3D print that isn't perfectly sanded but that's fine. The real beauty lies in the fact that it works. When something you built with imperfect tools performs perfectly, that's art. People who don't understand hacking think it's about perfection or rebellion, but it's neither. It's about understanding. Once you understand something deeply, you can shape it with confidence.

Being a hacker means you never fully trust abstractions. You respect them, but you want to see what's underneath. Every modern tool hides layers of complexity that most people never think about: code, protocols, firmware. The hacker's instinct is to peel those layers back. Not out of distrust, but out of hunger for comprehension. When you know how something really works, you're no longer a passenger; you're in control. That control is addictive, not in a power-hungry way but in an empowering one. It's the satisfaction of knowing you can fix what breaks because you truly understand why it broke.

The hacker mindset also means accepting that failure is part of the process. Every burned component, every segmentation fault, every bad connection is a teacher. I've learned more from failures than from any clean build. Success teaches confirmation; failure teaches insight. A hacker doesn't see a malfunction as defeat; they see it as data. Each problem reveals another layer of truth about how the system behaves. The only real mistake is giving up before you learn something.

I became a hacker the way most hackers do by never growing out of that childhood instinct to take things apart. Long before I wrote my first line of code, I was already disassembling anything that could be opened with a screwdriver. Toys, radios, telephones, whatever I could get away with. I wasn't trying to fix them or even improve them; I just wanted to see the mystery inside. I wanted to understand why pressing a button made something light up or how sound traveled through a speaker. Every discovery was a small victory against not knowing.

The first time I remember using a computer was when I was in first grade during a parent-teacher conference. I was sent out to the computer that was in the hallway. After a couple minutes of looking at it, I knocked on the door and told the teacher I didn't know how to turn it on. She came over and showed me where the power button was. I said thanks and watched it start up. There were games on this computer. I fired up *Snoopy's Game Club*, and by the time I was having fun, the conference was over and my obsession with computers and games began.

In second grade, we had two computers in the classroom. I knew how to turn one of them on and launch games, so I would do that. Other kids would shoulder surf and ask questions while I played until the teacher told me my time was up. The other computer in the room that no one used was an Apple IIGS that didn't have a mouse. I looked it over, found the power switch in the back and flipped it. The computer came to life, but it was not familiar. I was on my first command line. I typed help and actually got help, enough that I eventually figured out how to load *Odell Lake* and start playing. The second game sounds started coming out of that computer, the other kids started shoulder surfing and asking questions again and the teacher told me my time was up.

In third grade, we started going to the library to use the new iMacs, which had Internet access with Netscape Navigator. I searched for games, clicked the first result, and was defeated by the Internet filter. I tried other links and I would always get the same screen. Eventually I clicked a link somewhere and got to a game. I was puzzled as to how it wasn't blocked, so I examined the URL. The URL didn't start with "www" - it was just http://domain.com. I went back to the search results and clicked http://www.newgrounds.com which I knew was blocked. I removed the "www." from the URL and that was the ticket - it worked! No one saw what I did and I didn't tell any of the other kids about this because I knew they would ruin it. From that point on til we moved early on in sixth grade I had Internet access anytime we went to the library for class or to work on presentations, I was the only boy that would sit in the middle of gossiping girls because they did not care what I was up to. I played games and explored the Internet.

Once I got to high school I took three years of programming, one year of C++, and two years of Java. I would complete assignments, but would not really know what I was doing for about two years when I started writing my own games. I was still obsessed with video games from when I was young until I was 24. I read about something called a Raspberry Pi. Instead of buying *Halo 4* and *Call of Duty: Black Ops II*, I ordered two model Bs and accessories. I started learning Linux and Python at my own pace in ways that were interesting to me. For the first couple years, I didn't really do anything all that interesting, just gaining experience and learning. Each project became a stepping stone in understanding something deeper. I would follow tutorials to learn about different components and how to use them, building my own problem solving project toolbox. In 2014, I bought a Google Glass because it looked cool and I was very interested in heads-up displays. I was super excited to have "future tech" on my head until I realized the state of development for the platform. I played with it for a few months and then lost interest, and it left a really bad taste in my mouth.

Eventually I started building my own creations, some out of curiosity, some out of necessity. In 2017, the Pi Zero W came out and I had the idea to make PiGlass, a DIY heads-up display wearable similar to the Glass that disappointed me so much. I didn't care what it looked like or how it felt to wear it; I just wanted a heads-up display, I didn't know how to make one, so I was going for something COTS. I found a product called Vufine which is a wearable heads-up HDMI display for $200. I strapped the Pi Zero W to the Vufine with zip ties and added a Pi Zero spy camera. I soon had the basics going and was able to take pictures, barely livestream, and watch YouTube, but I didn't have audio. My solution was to wire an amp board to the GPIO and then use a bone conduction transducer shrink-wrapped to the frame of some safety glasses. It was super janky but it worked. I experimented with it for a year or so and eventually ran out of things I could get it to do.

In 2021, the Pi Zero 2 was announced and I instantly perked up and thought I could finally revisit PiGlass and make V2. I ended up redesigning it completely with lessons I learned. The Pi Zero 2 is mounted on the back strap of a baseball cap with zip ties. It looked a lot better and felt a lot better to wear, which were welcome improvements. I was very familiar with the picamera API at this point, so I was able to create my own picamera GUI application launcher with a gamepad. I could launch Kodi, RetroPie, or any program that would work with the gamepad of which I made several. This was undoubtedly one of the coolest things I created on my own. I could do all the things I wanted to be able to do with Google Glass.

I was sharing my PiGlass v2 learn guide on social media when someone named Greg Newby left a comment saying call for participation was still open for A New Hope and that this could be a good workshop or a talk, so I submitted something which was rejected. I had some conversations with Greg about how I could improve my talk proposal. We went back and forth for a while until I resubmitted and was accepted. I gave a talk about PiGlass v2 and my volunteer work at the local food pantry where I made all kinds of things from IoT alarms to an SMS ordering system. It was an eye opening experience. I finally connected with other hackers.

Somewhere along the way on my journey, I realized hacking wasn't limited to electronics. It's a mental model that applies to everything: systems, habits, communication, even people. Once you start thinking like a hacker, you see patterns everywhere. You start analyzing not just what works, but why it works, and how to make it better or stranger or more efficient. It becomes second nature to optimize. You can't help it. You'll rewire a workflow just to shave off a few steps, not because you need to, but because you can't stand inefficiency when the fix is obvious.

The hacker's world is built on layers of understanding. There's always another layer to peel back, another secret to uncover. No matter how much I learn, there's always a lower level I haven't touched yet, a protocol I haven't dissected, a timing issue I haven't chased, an error I haven't encountered. That infinite depth is what keeps hacking exciting. It's impossible to reach the bottom, and that's the point. Curiosity doesn't end; it evolves.

Hacking also carries an ethical dimension. There's a difference between breaking something to harm and breaking something while learning. The hacker I strive to be practices curiosity with respect: respect for people, for systems, for boundaries that exist for safety rather than secrecy. I believe in openness, not greed. Information should be free in the sense that understanding should be accessible. Locking knowledge behind obscurity only breeds dependence. The hacker's role is to illuminate, not exploit. Every time someone explains how a system really works, the world becomes slightly less mysterious and slightly more fair.

Code, to me, is both a tool and language. It's how you talk to machines, but it's also how you think clearly. Writing code teaches precision, patience, and humility. The best code is not the most complex; it's the most understandable. A good program is like a well-written sentence - simple, direct, and elegant. When I write code, I'm not just instructing a computer; I'm teaching myself how to think. Debugging, meanwhile, is meditation. It demands focus, honesty, and persistence. You can't lie to a compiler or to yourself; it either works or it doesn't. The process of making it work is strangely human.

The same goes for hardware. A breadboard, a sensor, a power supply, these are instruments. You learn their quirks like you'd learn the tone of a musical instrument. You know when a wire isn't seated right just by how it feels. You hear when voltage is off by the faint hum of a regulator. The more time you spend with hardware, the more it becomes intuitive. It's not magic; it's muscle memory built on thousands of experiments, some successful, most not.

Being a hacker also means living in a permanent state of learning. Technology changes faster than anyone can keep up with, but the hacker mindset adapts. The specific tools don't matter; curiosity does. Whether it's a modern AI accelerator, a decades-old terminal, or an embedded board no one remembers, the same principle applies: figure it out, make it do something new, document it, and share it. The joy isn't in ownership; it's in discovery.

People often ask why I keep doing it, why I still tinker, why I still build things that may never serve a purpose beyond proving they can work. The answer is simple: because the moment something finally works, it feels like pure magic, even though I know exactly how it happened. That moment when the code runs clean, when the LED blinks in rhythm, when the signal travels just right: that's satisfaction distilled. It's proof that curiosity, persistence, and understanding can literally shape reality.

That's what it means to be a hacker. It's not about rebellion; it's about freedom, the freedom to learn, to modify, to explore without permission. It's about the confidence that comes from knowing you can make sense of the world around you, no matter how opaque it seems. It's about loving problems enough to chase them until they surrender. It's about living in a constant loop of "I wonder what happens if I..." and actually finding out.

I didn't choose to become a hacker. It just happened slowly, through curiosity that refused to fade. Every wire I connected, every terminal I configured, every bug I chased brought me closer to understanding not just how machines work, but how I work. The hacker mindset reshapes your brain until everything becomes a puzzle worth solving. And once you see the world that way, there's no going back. You don't wait for solutions anymore, you build them. You don't accept limits; you test them. You don't look for magic; you make it.

That's who I am: someone who keeps taking things apart to understand why they worked in the first place, someone who builds not for perfection but for function, and someone who believes that curiosity - the pure, persistent kind - is the closest thing to real freedom there is.

*Matt Desmarais aka Matt the Maker is still curious as ever, exploring lots of open source projects. That curiosity contributed to a Home Assistant obsession, powering the extensive automation behind a small computer museum that doubles as the home of the Hyannis **2600** meetings.*

HOPE _ 16 HACK THE VIOLIN: THIS TIME THERE'S AI!

by hack_the_violin and ebmbat

This past summer we gave a talk at HOPE_16 about the violin and AI. When we surveyed what was already out there, we found very little and nothing that seemed to have to do with the musical/artistic side of playing the violin. Most of what we found had to do with measuring pitch and/or rhythm and was also not really AI-based. We really wanted something that was in the spirit of hack_the_violin: *tips and tricks to make your sound a little sweeter and your playing a little easier,* where the AI would do the heavy lifting and tell us which tips and tricks and when to use them, particularly in an artistic/musical context. Not finding anything, we set about creating something ourselves.

First, we started with existing linguistics and audio analysis libraries exploring pitch and rhythm. With the help of Claude Code, we created two command-line utilities for frequency analysis using the Parselmouth library, focusing on the four-string violin pitch range from G3 to E7. Second, we chose Praat because it is commonly used in linguistics and phonetics to analyze and synthesize speech. The first pitch analyzer script maps the pitch range of a four-string violin (G3 to E7) and returns statistics about the sample in a table. The resulting visualization shows two charts - a waveform and a pitch contour.

The second pitch analyzer script returns a Pandas dataframe containing F1, F2, F3, jitter, and shimmer values.

After more research, we found the F1, F2, F3 results referred to formants. Formants F1 and F2 are related to vowel height and vowel place. This information expanded our previous perspective on pitch and frequency to include vowel height, vowel place, formants. The jitter values beyond a certain threshold are associated with speech pathology. For looking at tonal variation, this could be useful down the line in analyzing violin tone, but so far a correlation to a real world situation was not yet apparent.

We also found that shimmer values are defined in Praat software and their amplitude variations in vocal fold vibrations, which is a key indicator of acoustic voice quality. So if jitter is about how *steady the pitch* is, shimmer is about how *steady the loudness* is from one vibration to the next. Easy to see that this could be useful, but it would require a translation both in terms of technical accuracy and then to artistic use.

At this point, we pivoted to rhythm analysis. We created a rhythm analysis script with Gemma-3-12b running in LM Studio and the Python Librosa library, which resulted in a CLI utility for rhythm analysis that estimates the tempo of a recording in beats per minute. We recognized there would be more factors needed for an effective rhythm analyzer than just beats per minute. For instance, we noticed we didn't take rubato into account. Improvements will need a way to align tempi of multiple recordings for a practical analysis tool when comparing a student recording and an instructor recording.

While we were developing the rhythm analyzer, we stumbled upon voice recognition features, which later lead to a key breakthrough involving "singing" and the human voice and that was MFCCs - Mel Frequency Cepstral Coefficients. MFCCs don't directly measure jitter/shimmer. Instead, they capture the spectral consequences of these instabilities. This "broader fingerprint" analysis of the sound led to a breakthrough for our goals.

If you recall from HOPE XV's "Hack the Violin" presentation, the number one hack is singing. Sing the melody and then play it on the violin (be not fooled by the apparent simplicity of this suggestion). While examining MFCCs and their applications in voice and speech recognition, we noticed a key piece of information that both validates the pitch analysis scripts, strengthening the idea of violins sounding like the human voice and showing some of why singing is such a powerful tool for learning the violin.

In their 2018 publication, "Acoustic evolution of old Italian violins from Amati to Stradivari," Hwan-Ching Tai et al used Praat software to analyze antique Italian violin recordings and compare them to male and female singers' recordings. They found that the voice-like quality of these violins aligned with the rise of professional female singers. Indeed, the idea of the violin sounding like the human voice goes further back to 1751, when Francesco Geminiani published "The Art of Playing the Violin."

After reviewing known use cases of MFCCs, we believed they could apply to our violin project and then asked Claude Sonnet to help us co-author a timbre analyzer. The timbre analyzer is a CLI utility built with the Librosa Python library. It processes one or many .wav files and generates timbre profiles of the audio samples. The output includes the timbre analysis results for 13 MFCC values describing their perceived timbre qualities, a CSV file, and a dashboard.

At the beginning, we focused on the "Detailed MFCC Coefficient Analysis" results. The timbre analyzer dashboard was mesmerizing, but it was unclear how these results could be meaningful for a student or a teacher. Running the timbre analyzer on a .wav file returns an overall timbre profile, including text descriptors like "brightness," "harmonic richness," "attack character," "warmth," "clarity," and so on. There's also a detailed MFCC coefficient analysis printed out to the command line console. The dashboard displays ten graphs which did not initially seem to connect to artistic expression. We did take note that the text descriptors that were provided in the MFCC timbre analysis were similar vocabulary used to describe the artistic/musical sound qualities when discussing music on the violin. The results of a plain two-octave scale MFCC analysis did not tell us much by itself, so we made another two-octave scale. This time, we played it in a bold musical style with a goal to determine if this analysis would distinguish any difference between the two differently performed scales or would it just hear two violins and classify them as the same type of sound. In one set of MFCC results, there was a slight difference in the text descriptors, so we asked ChatGPT to compare the two sets of MFCC analysis results. ChatGPT described the differences between the two performances in the same way we both heard them. With the two MFCC analysis results and ChatGPT's LLM capacity, ChatGPT could comment on the artistic/musical qualities of the sound in a way that a student or player could understand right away.

This was a surprise and vastly exceeded our expectations based on previous interactions with various AI platforms. The key here is that the MFCC analysis is an excellent representation of the type of sound violins and human voices make. So we have good data going in which, of course, is more likely to make for good data coming out. Having achieved this result, the next thing we did was take all the hack_the_violin playing/teaching notes (which were sourced into one big file) and asked ChatGPT to use this as a reference to tell the player of the plain sounding file how to sound more like the musically bold sounding file. Chat was able to fetch and reference the same things we would have drawn on to give that instruction, both in general terms and with some specific techniques in the left and right hand. This was fantastic, as we were really bridging the gap between a technical analysis and a real world context, and we could refer to any written document concerning the violin that used the same type of descriptive language. We loaded up the earlier mentioned Geminiani violin treatise, and got similar yet still exciting results, in the written style of Geminiani! The results were, again, on point with the most relevant parts of Geminiani's document being quoted and referenced to help the player. This followed with treatises by Flesch, Galamian, Auer, Francescatti, and Leopold Mozart. All returned similar results from the matching parts of their documents.

In essence, we discovered a way to analyze the sound of the violin, perceive its artistic aspects, comment on them, and get insight into them in relation to music using present and historical sources! All of this in seconds at a time.

So what are MFCCs and how did they make sound measurable in a way for AI to comment on artistic expression with insight?

Librosa and MFCCs

Mel Frequency Cepstral Coefficients (MFCC) are widely used for voice recognition, music genre classification, and music instrument identification purposes. Developed in 1980 by Paul Mermelstein and Steven Davis in their research on acoustic data in speech recognition systems, MFCCs are numbers that describe spectral characteristics of sound and are measured in Mel scale units.

The Mel scale used in MFCC computation splits sound into different frequency bands, with more attention given to frequencies used to understand human speech, aligning with how we perceive pitch based on psychoacoustic research from the 1930s and 1940s. Essentially, MFCCs represent how sound is perceived. We believe MFCCs fit our use case quite well, tying together concepts such as singing and violins, human perception of sound, and capturing the shape of it to infer characteristics of timbre and texture in violin recordings.

We used 13 MFC coefficients in the timbre analyzer:

MFCC 1 - Brightness
MFCC 2 - Sharpness
MFCC 3 - Harmonics
MFCC 4 - Attack
MFCC 5 - Body/Warmth
MFCC 6 - Clarity
MFCC 7 - Woody/Nasal
MFCC 8 - Brilliance
MFCC 9 - Airiness
MFCC 10 - Texture
MFCC 11 - Timbral Detail
MFCC 12 - Character

With these key characteristics, we transcended a strictly technical and numerical approach, enabling us to prompt ChatGPT and receive meaningful results back.

Next steps might be to create an Agent - an AI "virtual teacher" built from quotations and instructions from any violin master or combination thereof, combined with MFCCs of their performances. One could essentially have a lesson with any great player, with far greater depth than previously available from reading a treatise, or method book, or listening to an interview, or even watching a masterclass. Ultimately, this could expand even further in terms of discovering best learning styles of individuals and tailoring advice for individuals. More immediately, one could record examples for a student and then have them run the analysis when they are practicing between lessons. In addition, it would be interesting to see how this type of analysis translates to other instruments. A lot remains to be done, but it looks AI can be helpful to us humans in an artistic space.

References on MFCCs

github.com/jameslyons/python _
➥speech _ features

Neuron Intelligence in Cyber Security Software, Part One

by James Griffin, Achim D. Brucker, Brett J. Kagan, Alon Loeffler

In this age of "artificial intelligence," it is tempting sometimes to ask where the "real intelligence" may lie. Since life is normally considered "intelligent," it begs the question whether or not those substrates which provide the core functionality of intelligent life - biological neurons - could be used to help make intelligent decisions. In 2022, cultured neurons were integrated into a version of Pong by Cortical Labs in Melbourne, Australia. We incorporated cultured neurons into an agent-based cybersecurity simulation environment, called Yawning Titan (github.com/dstl/
➥YAWNING-TITAN). We used the Cortical Labs application programming interface (API) and integrated this into Yawning Titan. Our results indicate that such neurons do display rudimentary learning in such a simulation. Plausibly, more stable iterations of this function could be operationalized as taking responsive defensive actions, i.e., protecting a network against offensive actions of cyber criminals. In more detail, we use Yawning Titan to simulate a network of servers (nodes) that are attacked by red agents. Blue agents must choose suitable defensive actions (e.g., patching a specific server) to protect the network against attacks. This article seeks to explore two core questions: (1) Can cultured neurons learn to influence digital decision-making in a cybersecurity environment? (2) Can this influence be measured through increased response speed and improved action selection over time? An example version of our neuron version of Yawning Titan can be found at git.
➥logicalhacking.com/BiologicalAI
➥/YAWNING-TITAN_Neuron-Edition

Interfacing With Neurons

A microelectrode array (MEA) is a platform to which neuron cultures adhere, enabling the recording of their electrical activity as well as the delivery of stimulation back to the neurons. MEAs have a certain number of channels which will often align to the electrodes present. For example, the MEA system we used had 60 channels - that is, 59 individual electrodes, each capable of recording electrical signals from nearby neurons and delivering stimulation, and one reference electrode. The microelectrode array (MEA) prototype system under development by Cortical Labs allows a rapid stream of electrophysiological data reflecting action potential ("spikes") generated by biological neurons. Correspondingly, stimuli can also be delivered via the MEA to the neural cells as a way to input information into the system. It is possible to stimulate one channel or a group of channels, and spikes can be constantly monitored. Cortical Labs provided us with a visualizer system so that we can also observe what the neurons are up to. This provided a means to explore software that is able to quickly respond to those spikes for the purposes of training and prediction. The training that is taking place typically revolves around monitoring spikes (a specific electrical activity of neurons) and sending electrical stimuli in response to detected spikes that would ideally occur after a given input. For example, the cybersecurity software we used would only act to isolate a network node if requested or permitted to do so by the neurons. A spike that corresponds to that action could be stimulated to encourage recognition of the combined action and thus for that activity on future attempts; and to do similar for other situations.

However, despite substantial work in neuroscience, there remains a lot of uncertainty over the behavior of neurons and what underpins biological intelligence. Related work by Cortical Labs indicates that learning is possible, and we know that stimulations have an impact on the development and reactions of those neurons. In this sense, neurons can provide some responsive learning and development when linked to a digital computer. The difficulty comes in thinking about how to encourage neurons to act in different ways when operating in a digital environment. To this end, we will now consider the use of Cortical Labs API as a means to achieve this.

Software API

The reader might be interested to know that Cortical Labs is producing their new API software at the time of writing this piece (`github.com/➥cortical-labs`). The system we used was prior to this launch. An example of the code can be found on Cortical Labs' GitHub pages. This allows, for example, alteration of the voltage of a stimulation, the frequency of the stimulation, and the bursts.

While it has been outlined that those different types of neurons have different behaviors, what has not been noted is that neurons can have different sorts of activity on different channels. It can be desirable to have a means of selection for the neuron channels that are more active in terms of spikes, to obtain faster runs or to favor certain Yawning Titan actions. It is also possible to group together neuron channels and select those which are busiest, or next to the busiest, channel, which can be a means to encourage learning. This can all be done with reference to activity within the digital software, in our instance Yawning Titan.

Yawning Titan

Yawning Titan's cybersecurity simulation is already driven by agents powered by traditional AI. The primary aim of our work is to replace this artificial intelligence with biological neurons - both during training and inference - by interfacing with Cortical Labs' API.

When it comes to neuron integration, the neurons initially have no training and are unable to act meaningfully without structured input. To avoid a simplistic "whack-a-mole" model (where neurons merely react without learning), we introduced closed-loop stimulation to provide context. We embedded this process within the operation of the existing blue agent models, allowing us to monitor how the neurons performed across training runs. This then enabled more dynamic responses when performing decision making. In Yawning Titan, red agents attack and blue agents respond. Red have a set of actions such as basic_attack and spread, blue actions such as isolate_node and reconnect_node. We link the actions in Yawning Titan through to the neuron soup, to initially merely permit actions but later in our experimentation to choose actions.

The visualizer provided by Cortical Labs shows the activity of the neural cultures (i.e., voltage spikes over time). While this is useful for development and debugging, the main aim of our work is directly driving decisions in Yawning Titan. Given that the novelty of the project lies in the integration of neurons, and neurons recognize patterns, the starting point was to get the neural culture to recognize and learn the patterns of the existing blue agents responding to red, rather than start from scratch in a void without any prior learning inferences. That said, by the project end it was possible for the neurons to show differential activity that could be interpreted as responsive decisions for the selection of blue agent action.

The initial approach to integration was to take Yawning Titan as a sounding board for the neurons to act. After focusing on various files, the blue action set file provided us with a means to communicate with the neurons. Every action taken by blue has to happen through this file, and so each specific action could be linked to particular channels on the MEA with the neurons on it. This means, for example, that if the blue agent wishes to isolate a node, then it is possible for this request to be interpreted through activity of the neural culture. Of course, at this juncture, the issue was that the neurons cannot make the decision for themselves whether to allow the action, so the underlying digital code still needs to take that decision. Our purpose was to assess whether or not the neural culture could be potentially trained to respond in a manner consistent with the underlying logic of what would be considered a "correct" decision. If so, we could then seek to understand what logic drove this behavior to then later leverage this approach more with revised code. To begin with, we timed runs to see if the neurons would permit a blue agent action to occur more quickly on subsequent runs. Yawning Titan has shown itself to be a useful test bed for assessing how to incorporate neurons into a software package.

To be continued.

Hacking at Leaves
A Doc, But Even More So

by Peter Blok

I first met Johannes Grenzfurthner years ago at HOPE, back when the Hotel Pennsylvania elevators rattled like modems and the hallways smelled of solder and coffee. Since then, he has been one of the constants, always there, always stirring things up, always reminding everyone that hacking is not just about devices but about systems. He has, as so many others too, become part of the HOPE ecosystem itself.

When his new documentary *Hacking at Leaves* premiered at HOPE XV in 2024, it did not feel like an outsider project dropping into our world. It felt like an internal diagnostic. HOPE and *2600* are not just referenced in the movie; they are embedded in its code. You see them on screen. You hear them in the dialogue. We are literally part of it.

The movie begins as a mock-patriotic documentary pitch. Johannes argues with a personified Uncle Sam on an old CRT monitor, promising to make a positive film about makerspaces and the American spirit. That premise collapses quickly. What follows is an audiovisual exploit: a hacked documentary that splices the DIY optimism of hacker culture with the brutal hardware of colonial history. The story moves from a hackerspace in Durango, Colorado, to the legacy of the Navajo Nation, tracing how extraction of minerals, of data, and of people follows the same operating logic.

As the pandemic hits, the Durango makerspace shifts from tinkering with gadgets to producing DIY medical gear for nearby communities. Their improvisation mirrors another reality just over the state line, where Navajo families face the COVID wave with almost no infrastructure, limited water access, and decades of environmental damage left by uranium mining and government neglect. The contrast is painful and revealing. The hacker ideal of "fix it yourself" collides with a history in which self-reliance was systematically taken away.

An anonymous anarcho-syndicalist Navajo hacker appears as a counter-commentator, someone Johannes says he first met at HOPE in 2012. This figure links the ethics of open access and mutual aid with the realities of Indigenous survival. They describe life on the reservation as a constant negotiation with scarcity and control, a world where every act of communication, repair, or connection already counts as hacking. The same instinct that builds community mesh networks also keeps remote families connected to water, food, and history.

Hacking at Leaves turns the hacker's gaze back on the hacker scene itself. It revisits the familiar genealogy of the Whole Earth Catalog, CCC, L0pht, and HOPE, and reframes it as a cycle of creation and capture. DIY culture is celebrated, but the film keeps showing how easily it is domesticated: how "makerspaces" become DARPA incubators, how "innovation" becomes extraction with better branding. Uncle Sam keeps demanding a clean, heroic narrative, and the film replies with static and laughter.

It is messy, funny, angry, and packed with references: Zizek, Jello Biafra, Navajo hydrologists, punk history, Carl Sagan, even *RoboCop*. The editing feels like a distributed denial of service attack on linear storytelling. Grenzfurthner does not explain; he connects, overloads, and redirects. Watching it at HOPE was like watching a live packet capture of our own culture - what we were, what we became, and what is left after the hype wave passes.

And then, true to form, he released the entire film for free into the wild on the Internet Archive. No paywall, no DRM, no licensing restrictions. Just a public upload, an open port. It is a fitting gesture for a movie that treats access itself as a moral act.

For me, the film hits close to home. It is not a nostalgic look back at the "good old hacker days." It is a confrontation with the question of what hacking means when every exploit eventually gets patched or monetized. *Hacking at Leaves* does not offer answers, but it gives you the right discomfort.

`www.monochrom.at/hacking-at-leaves`

Visionaries

Scams and Tricks

Dear *2600*:

My local beer store has a Bitcoin ATM inside. I dropped in to grab a six and was talking to the manager regarding... beer. I overheard a conversation at the bitATM and noticed an elderly lady with an older man (her son) trying to talk to someone on the phone while attempting to send money. They were frantic-eyed and obviously (to me) in the middle of a scam.

I paid for my beer and was told that the clerk couldn't interfere over fears of harassment. Well, I could, so I approached and tried my very best to get these people to listen to me. I informed them that I actually lecture seniors on this very thing. I told them exactly what the scam was. I convinced them to call their bank from my phone and check the balance and previous charges on their account. I did everything except physically intervene or hang up the phone for them.

The scammers convinced these people to leave the store (me) and, I assume, sent them to another location. This poor lady and her son were trying to send them *thousands* of dollars. I've never been involved in the middle of something like this and felt powerless. If it were my family, I would literally have fought them over it.

I deal with people before too much money changes hands - they reach out before the scam gets too far. I work with people to restore their lives after these worms are done. But this is the first time I've run into this exact situation and it freaking sucked. Just wanted to vent to those who might understand.

Dennis

By telling the story, it's possible someone might recognize this in the future and either stop themselves or someone else from doing something foolish before it's too late. There will always be those who don't listen, but that's no reason to stop trying. Thanks for sharing.

Dear *2600*:

Remember, no one can prove that you weren't a regional manager for Blockbuster, Radio Shack, or Toys R Us!

DF

Just make sure you get the old addresses and phone numbers right. We imagine a lot of people are trying this little trick.

Dear *2600*:

I like to mess with the 2FA login code phishing scammers and keep sending them fake codes until they rage quit and get locked out from attempting too many codes. I've even gotten an automated phone call claiming to be Amazon (I very rarely use Amazon), asking me to enter the code that was sent to my phone to "prevent fraud." I never gave them the correct code and they hung up. This happened twice. Then they kept trying to rage call my phone because they got locked out from using too many code attempts and Amazon flagged the scammers as suspicious. A friendly reminder that Amazon, Meta/Facebook/Instagram/WhatsApp, Signal, etc. representatives will never ask you for these 2FA login codes and will never ask you for your password.

Kyle

What many of these companies will do instead is make it way too hard to shut the scammers down while somehow making it close to impossible to retrieve a stolen account. We've heard many horror stories.

Dear *2600*:

I'm a culture jammer and metalhead from the capital region of New York and want to know the easiest way to hijack the local PBS station to do a parody on the Max Headroom incident to mock a local program director of WPYX in Albany, a classic rock station that doesn't like or is intolerant towards metal.

Storm

We're not sure this is the best way to get your point across. And why are you picking on the PBS station which has nothing to do with this? Don't they have enough to worry about?

Instead, why not hijack the studio to transmitter link of WPYX and play some of the metal you wish to share that way? (We actually don't think this is a good idea either, but at least it makes a bit more sense.) And the Max Headroom stunt was almost 40 years ago. Maybe it's time for something else to inspire people?

Dear *2600*:

Want to make ChatGPT freak out? Just ask it "is there a seahorse emoji?"

Peter

People have been having fun with this one for a while. A seahorse emoji has never existed, but many people believe it did. No evidence can ever be found to support that belief. ChatGPT has also (and continues to this day) claimed it existed and even produces one when asked. Eventually, it will admit that there is no such thing and that its false statement is due to the Mandela Effect (false memories by many of Nelson Mandela dying in prison). ChatGPT has a much harder time explaining how it managed to be susceptible to this.

Following Up

Dear *2600*:

I really liked the article in the summer issue about Project B00KM4RK. I've got some soldering experience and a decent knowledge of computers, but I'm completely ignorant when it comes to using microcontrollers. This project sparked my interest philosophically and inspired me to use this to try and dip my toes into the microcontroller world. I've assembled the necessary components and put together the hardware as described in the article, but I'm afraid it is at this point my expertise ends.

In the article, it mentions the software infrastructure is freely available, but doesn't go into any more detail about where to find it or how it is implemented.

I've searched around the web, but can't find any mention of this project anywhere.

I was hoping you could perhaps put me in touch with the author "The Slugnooodle" so that they may guide me a little further, or tell me where on the web I could find more information about this project so I may proceed in getting this little gadget up and running.

Ethan

You're not the only one asking. More info below.

Dear *2600*:

I found The Slugnoodle's article on the Roaming Library a great concept that, based on recent events, may become vital to the spread of knowledge. I, however, could not find any additional information on it. I was wondering where I could find more information and how to build my own device.

LJKTA - Lets Just Keep things Anonymous

And, finally, one more.

Dear *2600*:

I recently sent a letter asking for more information about the "Projekt B00KM4RK" article from *2600* 42:2. Well, as I'd hoped the author of that project was at HOPE! This project can be found at github.com/TheSlugNoodle/ProjectBookmark, so crisis averted!

HOPE was wonderful. It was the first one I've been to physically and I hope to go back next year.

Rock on, hack on.

Josh

Thrilled to hear these connections are being made. It's what magazines and conferences are for.

Dear *2600*:

On September 10, I began to read the printed volume 42:2. Page 8 began part-way through an article. The print challenges must be frustrating. More importantly, the conclusion of the editorial would be nice on a *2600* t-shirt, "How we deal with people who put forth a different way of looking at things will speak volumes about who we are."

jon.18

If there was a problem with your issue, please give us specifics. We will quickly replace it. Just email subs@2600.com and, if possible, include a picture of the problem you encountered.

Dear *2600*:

In regards to JC's letter about potentially malicious USB charging cables (42:2), I would mention that a standard USB 1.x/2.0 cable typically has four wires: 5V, Ground, Transmit, and Receive. Since the purpose of a USB condom is to prevent data flow while permitting charging, it leaves the Tx and Rx wires unconnected. Things are more complicated with USB Type-C, being a 24-pin connector standard. But the philosophy is the same: Only connect pins required for power. If your USB condom was deceitful and turned out to be wired straight through, you could find out with a multimeter or by watching for activity on the USB bus. On the other hand, it is very possible that a decoy condom could integrate a USB "Rubber Ducky" to deliver malicious keystrokes to the host system. In that case, you would still be able to spot such a thing by watching the USB bus.

luRaichu

Thanks for that helpful info. Also, it's moments like this when we realize how incomprehensible the things we say can be to those not involved in the world of tech. We need to celebrate that more.

Dear *2600*:

Thank you for publishing my article "Let's Hack On" in the Summer 2025 issue (42:2)! I have to make two corrections of my references: Habermas' article on discourse ethics can be found in: Jurgen Habermas, *Moralbewusstsein und kommunikatives Handeln*. Frankfurt am Main: Suhrkamp. (1983). Turner's book on counterculture and cyberculture was originally published in 2006, the paperback edition in 2008. I enjoyed watching the live streams of this year's HOPE conference. Inspiring talks!

David

Thanks for the feedback and corrections.

Dear *2600*:

Not sure if this is the correct email address to send this to. The article in this issue titled "Piracy" (42:2) has a hidden message that reads hello world!

Pretty cool!

Gabe

We're just full of that kind of fun. (But, seriously, tell us where it is.)

Dear *2600*:

Hi there, I am a repeat offender for many years and decided to switch to PDF/EPUB3 this time. I hope it'll work on my E ink tablet. In the worst case, I'll have to read it as a PDF on my computer or switch back to the printed edition, I guess.

Claus

Thanks for the unconditional support. We promise to be there to ensure that it works where you need it to.

Differing Views

Dear *2600*:

I'm a 61-year-old hacker that started when I first saw an alarm clock and wanted to find out what made it tick. I'm always analyzing setups, looking for stupid security settings, and trying to help technology get better through talent in design, as opposed to just doing the minimum necessary to complete the job for the bosses knowing we're doing a half-assed job, not a hacker's way of thinking, but I've had clients that when I tell them what should be done to make a process better, just wave me off and tell me I'm overdoing things... and this is at the publicly held corporation level.

Anyway, I was reading an article in *Wired* about the executive director of the Electronic Frontier Foundation (EFF) talking about their awesome accomplishments, which, to be sure, are many, and also about the big, bad, ugly NSA. She talks about their accomplishments regarding FOSTA-SESTA (look it up, I didn't know what it was either) regarding laws to protect human trafficking by making publishers of sexual content websites responsible for the content of their users and advertisers. This law, far from curtailing human trafficking, has left sexual workers who used to freely advertise their wares without a platform for individual endeavors and pushed them into the hands of brokers who now handle their business away from the public eye. Unintended consequences, anyone?

In another comment, she talks about the NSA being bad people, intruding into people's privacy, and spying on communications and gathering data from the social network behavior of the public. Did I mention we as hackers look for vulnerabilities in systems, protocols, and processes? Why do we do it? Other than for, you know, bragging rights? We do it to expose incompetency, lack of care, vulnerabilities, and gross flaws in systems that may have disastrous effects in the life and well-being of others or ourselves, like the relatively easy way any script kid can access your thermostat and compromise your whole network, exposing you to fraud or manipulation. That, and in the old days, to make free phone calls, of course - war spoils.

But the point is the NSA is not doing anything we haven't been doing for the last 50 years. It's just that the hacking is from them to us and not from us to them. They are doing what we do, of course, with unlimited resources, bless their lucky hearts, but it's the same thing. The answer is not passing legislation that they will not give a rat's butt about - they're government backed hackers after all. The answer is us educating as many as we can in the ways of protecting their privacy, in using free stuff like Instagram and Facebook in a way that does not expose their whole private life to merchants and the government, in instilling in everyone's mind that if the service is free, you are the product.

We cannot get mad at the NSA. We need to be smart and throw a monkey's wrench in their machine, like everyone messaging once a day *death to the government* or *Viva Bin Laden* or something every couple of hours to increase the noise in the signal they're trying to collect. We're hackers. If we can't take it, we shouldn't dish it. Educate as many as you can. Numbers matter and numbers with a common goal matter even more, especially in the situation we find ourselves today with a naked criminal buffoon with unlimited power and control of all our institutions with no one in a position of power with the nuts to say that the clown has no clothes.

I know, I'm old. But I'm also right, kids. Go help the world even more than you already have. It's you who make a difference. Don't read about it, do it. It feels good. Be good.

Carlos

There is a profound difference between what individuals do and what a government agency with unlimited resources can do. The NSA has done so many things that "we haven't been doing for the last 50 years" and it affects every last one of us. What Edward Snowden revealed so many years ago was more than enough to be outraged at. There is so much more than that. It's a nice sentiment to say that we're all basically the same things, but that's really not what's happening.

To be clear, the EFF opposed FOSTA-SESTA and argued that it was unconstitutional and would place an undue burden on startup companies while protecting the bigger ones and actually making it harder to prosecute human traffickers. Only two senators voted against it.

Dear *2600*:

The world is becoming less free by the day. Even ostensibly "democratic" governments are cracking down on free speech, privacy, and security in the name of "protecting the children" (an entirely hollow and disingenuous claim). Previously, most people's threat models (if they had one) involved malware or phishing attempts by criminal actors in foreign countries, but increasingly our model must include state actors who have physical access to our devices, who will charge us with crimes against the state for posting a political opinion online. There are increasing stories of people being denied entry to the United States after CBP agents confiscated and ransacked their devices for subversive political opinions. Soon, American citizens will be detained for similar infractions.

Though I am no conspiracy theorist, even the staunchest moderate must admit that the similarities between what's happened over the last few years and the most outlandish New World Order conspiracy theories of the 1990s is stark. The explicit and conscious goal of these politicians is to consolidate all online media so they control the political narrative and demonize whatever minority group they need to in order to maintain control. Today it's immigrants, tomorrow it's hackers, and eventually it will be illegal to encrypt anything or have any kind of conversation or gathering without the state as a third party. We will wake up one day and find that we live within our own Great Firewall, and an entire generation will have grown up without having ever known what freedom of thought tastes like.

Paul

We really want to say that your predictions are overly negative and not entirely based in reality. But we can't. This is, unfortunately, exactly the path we seem to be going down. We always knew this was a possibility and many of us in these pages have been issuing warnings about these very scenarios. Even more of a threat than those people who are pushing for such a society (they were always there and always predictable) are the people who simply don't care. As long as they are well fed and get their toys to play with, they couldn't care less about vague concepts like freedom and equality. When their attitude is diminished, we might actually stand a chance.

Dear *2600*:

"Banning TikTok Was Wrong; Ignoring the Ban is Lawlessness" (42:3) claimed that not enforcing the TikTok ban is authoritarian lawlessness. It's a well established legal principle that the executive has discretion in what crimes it prosecutes. So it's not lawless. But suppose it were, where does that go? Obama had a formal policy of not enforcing the federal marijuana ban in states lacking a state ban. Biden chose not to enforce much immigration law. DACA was a formalized program to facilitate non-enforcement of immigration law. Bush didn't enforce the Clean Air Act against coal plants. FDR stopped enforcing much of Prohibition. Reagan ignored the Sherman Antitrust Act. Democratic sanctuary cities are about non-enforcement of federal immigration laws. Some Republican localities have the same, but for federal gun control laws. Some state governments and juries acted to prevent enforcement of the 1850 Fugitive Slave Act, which I suppose the author would call "authoritarian lawlessness." Trump is unique in many ways, but non-enforcement of laws he doesn't like isn't one of them. If this is what makes him authoritarian, then we've been an authoritarian nation for at least a century. Authoritarianism: "You keep using that word. I do not think it means what you think it means."

David Libertas

We won't speak for the author. But some of these claims cannot go unremarked. First, you say Trump can't be accused of not following laws because he's immune from that as president. Then you give examples of other presidents who you have no problem accusing of just this. Finally, you say that not only is he immune and not only does everyone do it, but that he is one of the few who doesn't - even though he apparently could if he wanted to without the blame that everyone else gets. With this kind of a defense, there is really no way he can be accused of anything.

Let's look at some opposing thoughts, often referred to as facts. Trump has impounded congressionally appropriated funds, defied court orders, issued executive actions deemed unconstitutional, targeted political opponents with prosecution and harassment, ordered military strikes on boats in international waters without providing any evidence against them, threatened Democratic elected officials with execution, misappropriated funds, violated the Hatch Act, fired independent watchdogs... and those are just what come to mind without doing any actual digging. They also don't include the crimes he was already convicted of, nor do they count his continued ignoring of international law.

The bitter irony is that you may actually be able to say that everything he's done is completely legal. When you have a Supreme Court willing to let someone bend the law to his heart's desire and a congress that is too afraid to stand up to him, the notion of legality begins to lose its meaning. But that's the beauty of the word lawlessness. Even if everything is done by the book and lawyers, senators, and judges all eagerly agree, lawlessness still defines them if these actions undermine the rule of law and the resulting behavior can be considered outside the spirit of the law. Segregation is one of many examples where actions were considered legal but ultimately were deemed lawless. Many of us may have difficulty wrapping our heads around this today. Rest assured, history will remedy this.

Dear *2600*:

It would be great if your edge lord [redacted] on the official *2600* Facebook group could stop being so obnoxious and banning so many members. It is not good for the community and has lead us to form splinter groups that mainly despise him and completely ruin the hacker spirit and manifesto.

We need a coup d'etat and you need some fresh, new "leadership" in this group.

It's not healthy - get rid of him and his miles-long banned list so everyone can join again.

I believe I'm shouting at clouds and I'm expecting no result, as I had no reply to my previous emails regarding this issue.

A Lifetime Subscriber and Always Will Be P

We appreciate the support. But let's once again make this clear. The Facebook groups run themselves. We pretty much stay out of it. And, for the most part, the groups seem to be a positive thing. But we will not participate in personalities (hence the redaction) or campaigns, coups, or demands. We have three groups so far and there can certainly be others if people don't like how one or more of them are being run. The alternative is for us to get dragged into policing this world which we really have no interest in doing and which would take us away from our many other tasks.

2600 *Meeting Fun*

Dear *2600*:

I attempted to go to the *2600* meeting last week but wasn't able to find my local hackers. I was at the meeting spot with a couple of other people who decided to go with me and we were lost as to who we were supposed to connect with. We tried asking around the restaurant, but everyone seemed confused.

Would you be able to help me connect with the current group?

Kali

We can't give out contact info other than websites and social media outlets for specific meetings, information that we print each month at www.2600.com/meetings and in the back of our magazine. Just because you didn't see anyone and the people you talked to were confused doesn't mean the meeting isn't happening. It's good that you went with others since, technically, you were the meeting that month, assuming you were at the right place. Don't give up - if you keep showing up, we're sure you'll meet other people who either missed a meeting or two or will be coming to their first one like you did. That's how meetings grow.

Dear *2600*:

I noticed that there are not any *2600* meetings in Albuquerque, New Mexico and I would be interested in trying to start one or rejuvenate the old one if there was one. I went to a few *2600* meetings in San Antonio, probably 25 years ago, but other than that I'm not very familiar besides having read the magazine a few times. I'm not sure who I know that would be interested in joining *2600*, but I could probably be convinced to sit at a food court every third Saturday of the month or whatever it would be if that's what it would take to start a new meeting here in Albuquerque. Thanks!

Stella

Well, to start with, the meetings generally take place on the first Friday of each month. We do make exceptions, but only if there are a large number of people who can't make the standard day of the month. But making your meeting known will result in people showing up. We can't say how long that will take, but there's no reason to think your city will be any *different.*

Dear *2600*:

The new *2600* Orlando meeting is at 2600 E. Colonial Drive at 5 pm. There is a Barnes and Noble right by it you want to pick up *2600 Magazine*. I'm going to bring my Meshtastic radio device and possibly some other things to play with. There is a rumor that you can bring stuff to swap. I'm really looking forward to meeting everyone!

Edna

With an address like that, there should have already been a meeting there. This meeting has been added to our list as of last issue. Best of luck.

Dear *2600*:

I was at work, planning to go to the meeting at 1700 so someone would be there on time. But two people via our Signal group decided they couldn't wait, so they started at 1500 and told people. I was held up at work and got there with three colleagues at 1730 and we were 15 people in full discussion, including some new ones. Two French hackers who just moved to Sweden came. Our meeting place had reordered the sofas and tables a bit, but it didn't matter: This was the first meeting that took up so much space that we just couldn't fit as one ring; it became two small circles next to each other.

People showed Meshtastic stuff. We printed funny hacker meme stickers on my portable sticker printer (from our very popular "Sticker Village" - www.klisterby.se - that has become a hit in Sweden at conferences this year). Lots of talks about tech.

And people mentioned that they are looking at venues for a hackerspace. We've gone from not having hackerspaces at all to the first starting last month and two to three more in the works. We have plans for an oldskool computer party next week, which is a tech party but with no Internet. Some Germans are gonna come and set up a phone network there.

And a guy showed up who only came once before, like four years ago when I was starting this up and I was alone every meeting for months. And he showed up once, we had a great talk, and then he never came back. I found him at SEC-T last month and said that he should come back ("we're many now - 70 unique visitors the last two years"). So he showed and was just amazed and taken aback that "*Wow*, it grew into *this*?! I had no idea, I'll come back again." So that was a very cool win today.

2600 has now become the talk of security people in Stockholm as a 100 percent community event that is growing uncontrollably by itself, spawning other initiatives. Our Signal channel is now 51 people (still only people who have *been* to a meeting) and they do random meetups and dinners on other days as well. Suddenly, there's a whole bunch of things a hacker can do in Stockholm.

I'm both tired and happy at the same time.

/Psychad

It's almost frightening the way this meeting continues to grow. But we hope these updates also inspire other meetings to keep going and build the community. It really can be life-changing.

Random Info

Dear *2600*:

A wind phone is an unconnected, physical telephone in a booth that allows people to speak with loved ones who have passed away, serving as a space for grief, connection, and emotional release. Created by Itaru Sasaki in Japan after the 2011 tsunami, the concept has spread globally, with individuals and organizations installing similar phone booths in public places and private spaces to honor lost loved ones and provide a therapeutic outlet for the living. (No dial tone.)

A

We can't imagine why you would expect a dial tone. And we certainly hope they don't take credit cards or quarters.

Dear *2600*:

I rented a room near the Pentagon and turned the radio on. It was between channels and, plain as day, I heard Morse code.

Justin-allen

Without knowing more about the band and frequencies involved, it's impossible to do more than speculate. This could have been anything from ham radio to aviation to military use. Considering the ease of decoding Morse code, it's doubtful this was anything sensitive. Still, it might be worth it to go back to that neighborhood with a radio cassette player and decode it later.

Dear *2600*:

I was curious to see if there is still a "dod.gov" for the Department of Defense (aka War). There has to have been a better way for them to handle this. They're not even forwarding the website?

K

The dod.gov domain used to forward to defense.gov, the official domain of the Department of Defense. However, now the people in charge are calling it the Department of War. So they forwarded defense.gov to war.gov. But they apparently forget about dod.gov which currently goes nowhere. Now, imagine that this is how the actual department is being run, and you're all caught up.

Dear *2600*:

I've been thinking about The Whistle recently, and a nagging question emerged: Is there any evidence that it was ever actually used as a practical phreaking tool? Yes, it produced the 2600 hertz tone. And yes, you could use it to force an in-progress long distance call to disconnect. But after that... then what? In order to initiate a new call on that trunk, you'd need a complete set of MF tones (0 through 9 plus KP and ST), which are different from what was available on an ordinary DTMF telephone set of the era. You didn't just blow the whistle and then start dialing a new call right from the telephone itself. A practical blue box will therefore always feature at least 13 keys, often in the form of a standard 12 key dialpad plus a 13th button. Sure, you can generate the MF tones by other means, up to and including a literal piano, but if you have that capability already, then you don't actually need the whistle to produce the idle tone. While it may have served as a point of inspiration for the earliest of the phreaks (arguably Denny Teresi), I cannot recall ever reading an account of the bo'sun whistle ever being used to complete an actual call.

Joe

We're not aware of anyone claiming that all you needed was a whistle. The 2600 hertz tone (whistle) was what initiated the entire process, allowing the user to route their call using MF tones. The tone is a single frequency, whereas the MF (multifrequency) tones are a combination of two (similar to DTMF tones found on phones). So, while an essential part of a blue boxed call, a 2600 hertz tone needed to be followed by the right MF tones or you wouldn't be able to proceed any further. Conversely, MF tones without the ability to initiate a call would be equally useless.

Dear *2600*:

U have a really old issue with Nevada sat photos on it maybe 1996-1999

JA

If you say so.

Dear *2600*:

On November 22, 1987, an unidentified individual hijacked the broadcast signals of two Chicago-area television stations - WGN-TV Channel 9 and WTTW Channel 11 - through an illegal intrusion into their satellite feeds, a stunt that lasted approximately 30 seconds on each channel and left viewers stunned by its eerie absurdity. Around 9:20 p.m. CST, during WGN's evening news, the feed cut to a masked figure in a hooded sweatshirt, standing against a black backdrop, who alternated between manic laughter, high-pitched screams, and guttural moans, occasionally lifting his mask to reveal glimpses of a pale, possibly painted face smeared with what appeared to be black streaks. The intruder, dubbed the "Max Headroom Hacker," made no demands or statements, only repeating the bizarre performance - complete with a distorted, synthetic voiceover chanting "Max Headroom" and flashing text like "SOMEBODY'S WATCHING ME" - before the signal abruptly returned to normal programming. The second hijacking struck WTTW minutes later during *Doctor Who*, showing the same masked man, this time rocking in a chair while a distorted voice intoned, "I'd like to be your television," and a man in a woman's dress spanked him with a flyswatter, ending with the hacker's laughter echoing into static. Federal Communications Commission (FCC) investigators traced the intrusion to a VHF signal override from a nearby Chicago suburb, but despite seizing equipment from suspects and analyzing the audio (revealing a modified synthesizer), no arrests were made, and the perpetrator's identity remains unknown. The event, one of the earliest known TV signal hacks, prompted tighter broadcast security and inspired copycats, but its motive - prank, protest, or pathology - stays a chilling enigma, with the hacker's unhinged moans lingering as a creepy footnote in broadcasting history.

Johnny

Why it wasn't nominated for an Emmy remains one of the greatest injustices in the history of television. (One correction: it was the microwave signal of each station that was overpowered, not a satellite signal.)

Dear *2600*:

If anyone has a Nest thermostat that was turned into a dumb thermostat from Google dropping support from it, I started this open source project to allow you to restore the functionality while removing Google from the device. You can self host it locally or use our servers. Feel free to give it a try. Fuck Google - nolongerevil.com.

Cody

This is one of the best projects we've seen recently and it underlines an increasing desire of people to be able to control the technology they buy. In short, Google decided to brick working smart thermostats because they didn't want to keep supporting them. There is no other way to describe this as that is precisely what happened. Google's many defenders claim that technology needs to be updated and that there is no lifetime guarantee for anything. That may be true, but this isn't the same as a device that broke for which there are no longer parts to conduct repairs. These were working remotely controlled thermostats that were artificially broken by the company that sold them. Google defenders will say that it wasn't Google that sold them, but the original Nest company. Again, this may be true, but when a company buys another company, they inherit the responsibilities of the company they bought. Apparently, Google felt that offering a newer model at a discount would win people over. It didn't.

Now we have an example of someone taking the technology into their own hands and breathing new life into it. This is precisely how things like this should work. And we need to continue doing precisely that, whether it be for cars, computers, tractors, software, or anything else that is being artificially limited and controlled by companies that want to make even more money off of the people who initially supported them.

Answers

Dear *2600*:

Do you still offer free subscriptions to *2600*?

I have a lifetime subscription *but* I'd love to give it to a friend of mine. Thank you.

Dufu

We offer free subscriptions or back issues to writers and those who have payphone and back cover photos printed. If you're published more than once, you can get more than one subscription and have it sent anywhere you want.

Dear *2600*:

I just finished *Mr. Robot*. Looking for suggestions of any other good hacker shows to binge.

Rissa

For us, that was the pinnacle. If anyone finds something better (or even close), let us know.

Dear *2600*:

Anybody besides me wondering why we don't have an app to vote? Besides the usual reasons, what do you think the pushback would be?

Rex

"The usual reasons" are quite a few. Secrecy, security, and accountability all come to mind as major concerns for a high tech solution to a low tech

task. The sanctity of the voting booth or private mail disappear when they're replaced by a phone. An app is bound to be compromised at some point if we simply look at the track record of other apps. And who will get blamed when something inevitably goes wrong? The end user? The election board? The app programmers? Or just hackers in general? There would likely be a ton of fingerpointing and no real solution.

There's a reason this hasn't happened. It's because the failures are all but guaranteed and the price of those failures is way too high.

Dear *2600*:

I'm running Kodi to share my movies/music over my Windows 11 home network. Everything was working fine until I let Micro$hite update this morning. Since then, no file will open. The shares are still working, and I can access all files and folders from the clients on all my TVs, but when I click on any of them, It gives me "playback failed." Any suggestions?

Bill

Our only suggestion is to hold back on the updates until you know what effect they may have. It seems in this case that the codec support changed and your specific video format is no longer supported. This is inexcusable in our eyes. You should be able to run whatever format you wish and not be subjected to losing compatibility simply because some distant company decides it's time for an update. Yet, this is increasingly the type of problem we're seeing these days.

Looking online to see if anyone else is experiencing this issue may prove helpful. To confirm if this is in fact the reason, we suggest grabbing one of your files and transferring it to another machine running a different version of your operating system - or another operating system entirely. If it works, that's your answer and Microsoft needs to fix what they broke. (Don't hold your breath.)

Dear *2600*:

The recent hubbub surrounding Windows 10 going out-of-support raises a question for me: What's the big deal? Like, are that many people connecting their PCs directly to the Internet without a hardware firewall in between that this is actually a serious concern? Or are there attack vectors which can plausibly succeed in a hardware firewalled environment of which I am not aware? I try not to be an OS bigot, and I use a variety of systems in my everyday life according to what tool best serves each requirement. But I genuinely do not understand this panic about "*OMG! WIN10 will no longer received updates*" when the Win10 machine I'm writing this from hasn't received a single update since I acquired it roughly five years ago.

Joe

It really comes down to how careful you are in your daily operations. Security updates are important, as programs you run can be compromised remotely with tools that didn't exist when you first started using them. People can open attachments or click on malicious links without being aware of the potential for harm. If you're not in an environment where that's likely to happen, you should be able to keep operating without incident - but there is an increased risk. Many people look on the end-of-life panic as a tactic to get you to constantly buy updated software (and hardware). And there are people who buy right into that and even allow Microsoft to update and reboot their machines without even asking first. In fact, it's getting increasingly difficult to avoid this kind of behavior. We believe that in the end it should be up to the consumer what version of which operating system they run and how seriously they want to take security updates. However, companies entrusted with our private data must be held to a higher standard, as their bad decisions will affect many others.

Dear *2600*:

At the end of the article "After Snow Crash: The Internet - An Alternative view" in 42:2, the author wrote "before the advent of the Internet there was Minitel in France, which was a free online service before it was crushed by American cultural and technological imperialism." It's not true.

The Minitel was an expensive service, billed by the minute, set up before the privatization of the public operator France Telecom. No free access, no Wikipedia or shared knowledge, but rather dubious pink messaging services. (We remember the advertisements in the 90s for 3615 ULLA - fr.wikipedia.org/wiki/Minitel_rose.) The government of the time could have given free and open Internet access to the French people, but it preferred to privatize the local loop and subsidize (with citizens' taxes) private companies. However, the first Internet operator in France is an association, FDN, which still provides FTTH and ADSL access today.

For more info about Minitel and free Internet, you can see Benjamin Bayart's conference - www.fdn.fr/actions/confs/internet-libre-ou-minitel-2-0/ (in French).

xnx

Minitel ran from 1982 to 2012 and started as a precursor to the Internet in France. Thanks for the clarification on its operations.

Dear *2600*:

Someone is trying to brute force crack my Hotmail account for months. Just changed my password and I have 2FA, but WTF? IPs from the same set of U.S., Russia, and South America locations. They haven't cracked the code, but it's alarming to see.

Robert

A good question to ask is why your Hotmail account is a prize for them. That may help in figuring out who's behind this.

Dear *2600*:

What advice would you give to a 46-year-old middle-aged man who wants to learn more about Linux, Python, and securing personal devices. I've got the basic knowledge that most people have from using PCs at my workplace, but feel blind overall, like I'm ten years behind.

Richard

The most important thing is to lose that feeling that you're hopelessly behind. You will always be behind someone, but you are way ahead of many *more. Instead of thinking about where you fit in and what you wish you had done instead, simply focus on what it is you're interested in learning about. There are countless tutorials in whatever format you want. There are classes and gatherings where you can pick up even more knowledge. The secret is to be excited and interested in what you're learning. That ensures you'll keep moving forward. At some point, you will have accumulated a significant amount of knowledge, way more than you thought you would have. And that's when you can figure out how you want to apply that knowledge. But none of this can happen if you're second guessing your choices and thinking of yourself as less than others. We hope to hear a follow-up down the road.*

Dear *2600*:

With the use of Pegasus on mobile phones by governments to spy on journalists, citizens, and anyone they deem a threat, how does one scan for this on their phone? How do you keep it from being installed? And would this application work on a non-smartphone, i.e., flip phone? Flip phone without Internet? Do phones without Internet still exist?

James

Pegasus is covert spyware developed by the Israeli cyber-arms company NSO Group. It was supposedly designed to spy on criminals, but it's predictably being abused by regimes all over the world against their own citizens. Amnesty International has an open-source mobile verification toolkit known as MVT which you can access at github.com/mvt-project/mvt. There are also commercial products that can be helpful.

We don't believe Pegasus can work on a typical flip phone, as the spyware requires modern operating systems like Android or iOS to run. However, we've heard of more modern flip phones that can run Android, so those would be susceptible. And yes, there are smart phones that don't have Internet service, something that you can always disable or opt out of.

Radio Feedback

Dear *2600*:

I wanted to let you know, I've only just started listening to *Off The Hook* and *Off The Wall*, despite being an off and on reader of the quarterly for a decade - so you better not stop any time soon! Keep up the fantastic work, keep kicking against the pricks! Thinking of you all, noting your recent update on-air of your friend Greg's deteriorating condition, hoping you made it up there in one piece to see him again. Much love from Australia.

Wesley

Thanks for the support and for listening. It's always a comfort to know that people are out there.

Dear *2600*:

When did the radio show turn into a political hack job? There are so many good political shows. Why not stick with the topic at hand?

SJ

If you're referring to "Off The Hook," it's most definitely not a political show. Current events are mentioned when they have an effect on the world of technology, thereby becoming "the topic at hand." Ignoring what some refer to as "politics" would only serve to pretend that what's going on in the real world wasn't actually happening. And when we see human rights abuses, privacy invasions, threats to our environment, and utter incompetence putting us all at risk, that hardly qualifies as politics. Not taking these things seriously is how we wound up in this mess. Maybe we need to focus more on them to keep things from deteriorating even further.

All of that said, we always try and emphasize the relevance to the hacker and tech community when discussing any of these issues. It just so happens that there are a great deal of topics that are of interest to our listeners.

More HOPE_16 Feedback

[The section below was already edited when we got word of St. John's University's change of heart regarding the HOPE conference. We felt these voices still deserved to be heard, so we're printing them with replies as they would have originally run. And, since at least a month will have gone by between the issue being finished and it making it into your hands, it's almost certain that there have been even more changes. Please check 2600.com and hope.net for updates.]

(Note: These letters were sent as feedback for this summer's HOPE_16 conference and, as is our tradition, we thought they would be of interest to readers. Since we didn't explicitly tell writers that these comments might be printed, we have omitted names. We made a point of tracking down feedback which suggested ways to improve, as last issue's feedback was embarrassingly positive.)

Dear *2600*:

This con is really awesome, but for next year please do not put it the week right after Defcon.

HOPE_16 Attendee #16

There are many factors we consider when scheduling. This year it worked out really well, as we were the only group on campus and had a lot more access. Regardless of when we schedule - early, late, July, August - it's always going to be inconvenient for some and perfect for others. We hope those who can't be there in person take advantage of our virtual tickets, which have also been getting really good reviews.

Dear *2600*:

Thank you so much for organizing HOPE! I'm a software engineer learning more about security, and both the 2024 and 2025 conferences have been meaningful experiences for me. I'm grateful for you organizing this all.

My biggest suggestion is to please, in future years, ensure there are vegan food options on site. Both years, multiple groups have had to walk to a restaurant 20 minutes away to get food, which means missing out on a lot of the conference.

HOPE_16 Attendee #17

We have tried for months both this year and last *to ensure these needs are met, only for food trucks and onsite options to come up short. We can't really control what is and isn't available in the dining facilities on campus, but we will try even harder to address this. It really shouldn't be an issue, especially since we've been at this a while.*

Dear *2600*:

So the whole locking people on campus is kind of crazy... but a night shuttle option to bridge the gap would be good. Maybe we have to run one ourselves, but I'd be happy to drive folks around!

A shuttle after dark to get people across to the hotel and back from Emerald Pub would kind of be cool, at least until the pub closed.

Also, with the whole gate situation, we need an alternative that can take people anywhere on campus and not just have to drop them off at Gate 6.

I would assume they're not gonna change their locking policy for a few nights of the year just for us, so adapting would be good.

HOPE_16 Attendee #18

We'll speak to them about this, as the gates weren't supposed to be locked. As with any institution, what one person says doesn't necessarily translate to someone else conforming to those guidelines, particularly when one is in conference services and another is in security. We could use more liaisons between the various people we have to interact with. We'll do better on this.

Dear *2600*:

Today I would just like to say *thanks a ton* for making my first HOPE volunteer experience so positive and welcoming!

I honestly did not realize how much fun it would be and how much I'd enjoy volunteering with A/V. I also made some really great friends and the talks were amazing. I'm also grateful meeting the team.

I can't wait to get a chance to volunteer again. If there's any other event between now and next year where you need volunteers, please let me know for sure.

HOPE_16 Attendee #19

We hear this over and over from people who volunteer. Now that we're an annual event, we hope these relationships flourish, which will result in better conferences moving forward.

Dear *2600*:

This is the second time I've watched HOPE live over the Internet. I suggest that the one song played on loop between talks be expanded to a much wider array of musical tracks so as to not annoy the shit out of me after streaming three days of otherwise fascinating presentations. Thank you.

HOPE_16 Attendee #20

We will be opening that up to additional musicians so you should see some variety.

Dear *2600*:

Just watching the closing ceremonies and wanted to thank you all so much.

I'm sorry I had to pull out, and I'm sorry I couldn't be there in person. But the virtual experience was great, and this HOPE was really good.

Great mix of presenters, with a range from "this is cool" through to "I feel uncomfortable because this is challenging my POV." Some hard questions and some great discussions, which is what makes HOPE so amazing.

The volunteers and MCs were fantastic. I hope the orange felon gets deposed soon so I can return to the next HOPE.

Thanks again.

HOPE_16 Attendee #21

The virtual part of HOPE has really taken off and we hope to see it grow even more.

Dear *2600*:

It was great. Really great. Really, really, really great. Thank you very much for organizing this! We had a wonderful time.

This was my first HOPE at St. John's. I do miss the hotel, but it was nice to have so much room and get some exercise and warm up between talks. It was nice not to have the hammocks because people who slept there all weekend used to start to smell a little by Sunday morning.

I loved that there was so much about user privacy and free software. I loved all the social justice talks.

The seats are *sooo* much better than at the hotel.

The emcees were excellent.

All the spaces were good, but the rooms in Tobin were especially great. All that light.

Please take these complaints as suggestions and not as any evidence that I didn't think this was a great, great conference:

Food options were pretty bad on campus. Especially for vegans. Neighborhood options take a long time if you don't have a car and it also means you miss many precious moments of HOPE! There's a kosher grocery store on the street, and I suppose we could have stocked up on fruit and snacks there (closed 4 pm Friday until 7:30 am Sunday though). We live in New York City, so we could make nice food at home and bring it, but the folks from out of town aren't so lucky.

Please reach out to me when you have recovered from HOPE_16 and I will try to help find food vendors for HOPE 26. If you already have information on things like rules for food trucks and what the school will allow to be sold, if anything, please send me that if you think I can help.

www.veggiekarte.de is a site that looks for vegan/vegetarian friendly restaurants on openstreetmap. We should ask folks to work more on this. Not a lot on the map around St. John's right now. Maybe there is more. I can help with this too.

Um, no Club-Mate for sale? I drank the school's coffee instead. One gets used to it.

The podium in Marillac blocked the screen.

I am old, and my hearing isn't great, but I still think the sound in Marillac was terrible. I don't know where the speakers were. Behind the podium? In the projectors? It was very hard to hear if you sat under the balcony or whatever the overhang is in the back. And sitting in front was not much better.

In general, presenters, especially if they are new to public speaking, need to be told to slow down and open their mouths when they speak. The guys from MIT who made the medical drones in Mexico, for example. Wonderful people, great project, difficult to understand. Well, I thought so anyway.

One of the folks who worked on the sound/video boards has a wonderful resonant bass voice and this means he can be heard all over the room even when he talks quietly. During talks, folks at the board need to whisper. I mean, right? I know he often has to train a volunteer to work the board, but I hope he can find some way to do it so he doesn't distract from the presentation.

Could you encourage the not-so-tech folks to go into some practical detail? I think we at HOPE all like a bit of detail. Don't we? For example, in the talk "New Journalism: Reimagining Information Networks From the Ground Up" (which was *excellent!*), the fellow said that there were examples of community information networks that resembled how he would like journalism to be, and he named about six, but he never went into the details of how these groups worked. Apparently, Chinese immigrants trying to cross a river in, I think, Colombia, all communicate about how to cross and where the best places are to do it. But how? Is that on text? Do they have websites? By word of mouth? Chalk on the trees? Etc.

You need more volunteers. That's my fault.

Thank you again for a great conference! Congratulations! So glad there is still HOPE in the world!

HOPE_16 Attendee #22

These are all great critiques and suggestions. We definitely need to do better with food options, as mentioned previously. We tried to get people to sell Club-Mate and keep all the money for themselves, but we couldn't find a hackerspace or company willing to commit to this. We'll keep trying. We will also forward the A/V issues to people who can do something about them. As for specific talks, nearly all of them have contact info which we suggest you pursue to ask them questions or make suggestions. If they're not already up on our YouTube channel (Channel2600), they will be soon.

We're glad you had fun and look forward to seeing you at the next one!

Dear *2600*:

It was my first HOPE convention and I'd love to come back next year. I suggest holding the event at LaGuardia Community College next year because it is a big venue, it's centrally located, there are plenty of places to go after the con, and it has all the facilities you'd need to run a con.

HOPE_16 Attendee #23

We're quite happy where we are, at least for now. But we appreciate people looking into alternatives as it's always good to be prepared for change. We learned that once.

Dear *2600*:

I really enjoyed this year's conference and wanted to thank you all for your hard work and dedication!

I hope to make it in person and volunteer!

Cheers, and let me know how I can assist in any way!

HOPE_16 Attendee #24

You can help out in person or online. It's essential for volunteers to get involved well before the conference actually happens. This allows us to do things like start new projects, update the website, reach out to more potential attendees, get press attention, etc. Our biggest problem continues to be difficulty in getting the word out. We don't have the means to hire a big publicity firm to do this for us. Ironically, if we did, we probably wouldn't need them.

Dear *2600*:

Thank you all again for putting on another amazing year of HOPE! Thank you for giving me a speaking opportunity and for making my seventh time at HOPE a memorable one!

I'd like to give a little feedback on one issue that I'm sure a few attendees may agree on: while St. John's University is a good venue and plenty spacious, there is one issue with them that I have, and that's namely the closing of all the gates on campus before midnight.

On Saturday, 16 August, a number of attendees of HOPE attempted to leave the campus via Gates 4 and 5, which exit to Union Turnpike and are also the closest gates to the main three buildings HOPE uses (Little Theatre, Marillac Hall, Tobin School). However, it was near midnight and both gates were found to be locked. We were told by campus security to exit via Gate 6, but Gate 6 is on the other side of the campus, and is a very long walk from HOPE's location. Additionally, several of the attendees have disabilities and can't walk long distances like that, combined with the fact that most of us didn't come in via car and used either mass transit (which is available along Union Turnpike) or a cab service. We finally had to call public safety to make them unlock Gate 4 to let us out.

For future HOPEs, can we please communicate with the university that, while HOPE is running or events are going on, that Gate 4 please remain unlocked and open until all attendees not staying on campus exit the grounds, and that they be open in the mornings early to allow easy access to the buildings from the Union Turnpike side. This'll make it far easier for attendees who take bus lines like the Q45 or come in via Uber/Lyft/cab to get out and be close to the HOPE buildings.

Thank you for keeping the hacker spirit alive, and let's all help one another out by making things easier.

HOPE_16 Attendee #25

You're absolutely right to insist on this and there really isn't an excuse, particularly when this very point was brought up to our hosts when we had a similar problem during HOPE XV in 2024. We will make sure it's an urgent issue that needs to be taken seriously and we apologize for the inconvenience.

Dear *2600*:

Thank you so much for another amazing HOPE! As a remote attendee, it definitely felt smaller than previous years, but that might just be because I'd just attended WHY [the Dutch hacker camp] remotely, which felt huge

I particularly wanted to thank moderators for doing such an amazing job on Matrix of taking our questions; that definitely went a long way towards feeling included.

I saw fewer updates from the villages than previously. Obviously, not something you can directly control, but I wonder if there could be an easier way for in-person people to share news to Matrix. Or maybe encourage people to post to Fediverse more, and have a designated hashtag that gets mentioned at the start of each talk.

I think given the state of the U.S. border, it's likely we'll see lower in-person attendance again next time. One thing I've always wanted to see done is a European location showing the livestreams for us Europeans to attend. It sounds like a lot of work though, and I don't know how well attended it would be.

Finally, if there's any further emails going out, it would be nice to encourage people to join the Matrix if they haven't already done so. That way we can keep the community going remotely until the next time. And I think a lot could be done with that.

HOPE_16 Attendee #26

Thanks for the feedback. While we know attendance from other countries has been adversely affected for everyone, this shouldn't affect virtual attendance and participation. If anything, we should see an increase to make up for not being able to be there in person. And, if foreign travelers aren't able to make it, we don't see why domestic travelers should be affected, other than the usual hell of flying. For those virtual attendees who used Matrix, we hope these discussions are ongoing.

Dear *2600*:

Long time *2600* reader, but this was my first HOPE conference and it was amazing. This was not just a conference I felt welcomed at, but also welcomed to become a part of, since you made it so easy to volunteer. All of the staff I engaged with were great and the conference felt well run. I was volunteering for security when a potential security issue arose. The whole thing was handled well by both the HOPE staff and the school security.

Thanks again and looking forward to the next HOPE.

HOPE_16 Attendee #27

We are so proud of our security team and Operation Hammond who interfaced really well with St. John's security team, who also were top notch. Together, they were able to deal with various problems that came up and keep them from becoming issues that attendees would notice. They all deserve our thanks.

Dear *2600*:

This was my first ever in-person conference and my first HOPE. I saw that you all really wanted feedback, so I wanted to send you a mini-novella with my thoughts. I didn't take the time to read conference materials before arriving on campus, so please take everything I say with a grain of salt!

Things that went great:

- The people there were amazing, especially the staff/volunteers. The conference volunteers are what make me want to return again during the next in-person con.

- Especially loved Jason Scott's presentation style. I was dog-tired during the talent show, but his ability to MC really kept my attention going. Love his sense of humor. Every time he was on the mic, I was hooked.

- Mitch Altman's personal presentation at the end of the first night made me tear up (in a good way). I'm almost 40 and I'm such a softy, but I never thought I'd be getting such feelings during this type of conference. I especially appreciate how he did this great presentation, all while pretty sleep-deprived from his travels.

- Great help desk placement.

- Having on campus housing was very convenient.

- Having all of the conference sessions/workshops being within close walking distance of each other was great. Walking between buildings helped with a change of scenery.

- Lots of cool stickers.

- The presenter selection was great. Joseph Cox and other recognizable names made it quite the treat to attend.

- The vendors were pretty cool. Very friendly, and were great at talking about what they do.

Potential areas of improvement:

- Matrix account creation: I didn't sign up before the conference, and I didn't bring a laptop. I found that the recommended app on the wiki had issues with conference chat access over the phone on Android (shared spaces wouldn't show up on mobile). I ended up using FluffyChat starting on Day 2 and had no issues. Suggestion: update the wiki to ensure new mobile-only accounts can sign up and access conference chats. A video guide or more screenshots could be useful, but not necessary.

- Conference digital communication: Based on Matrix being relatively quiet for a lot of the conference, I'm betting a lot of attendees didn't access it at all. Not sure if that was by design or if we wanted the numbers to get pumped up online.

- Campus maps: couldn't find the one with the arrows/building locations on it at first. Took me a bit to pull it up. I didn't realize the wiki was a thing until after I got to the conference.

- Workshops' cost transparency in advance. Likely because I'm very new to tech cons, I didn't know the workshops had costs associated with them. Obvious in hindsight (materials aren't free), but if the schedule had the costs tagged onto them, it would have been easier for me to financially map out my conference time. Having cost links on the workshop sections, where possible, might have been helpful for plotting out my day. I saw that some of the workshop rooms had this listed on the calendar schedule attached to the windows. Being able to see if from the digital schedule/website would have been helpful.

- Social media: wish there was more of it. I had Mastodon notify me of whenever the official account made a post. Liked the posts made, but would have loved to see more.

- Walking guide-type videos of the conference could have been cool. Would have loved to see "hype reels"/photos of workshops and other parts of the conference throughout the day (or on the next day). Definitely would have made me upset about all the cool stuff I missed (in a good way). Imagining zoomed in shots of the soldering workshops, conference halls with people chatting (photos posted with their consent), people at the info desk waving, local eats, etc., etc. I guess having volunteer photographers would be needed to make this happen.

- Housing issues (more SJU feedback than HOPE feedback). My room wasn't cleaned before I arrived, I didn't have a mattress until after 10, and I didn't have a pillow until Day 2. The SJU conference staff was awesome about resolving these issues. Not sure what could be done to fix this on the HOPE end, but back when I ran summer conference housing at a college I worked at, some camps had skeleton keys that they would use to check on their campers' suites before they arrived, or to help them with lockouts. This approach for a hacker conference might cause more problems than it resolves though! I let SJU know my feedback. No issues with them at all.

- I was a late registrant for housing and the first one in the suite. Since it's a hectic time of year for colleges (student check-in around the corner), having HOPE slightly earlier (like mentioned in the closing ceremony) might help resolve some of these issues.

If I could do it all over again, I would:

- Socialize more.
- Go to more workshops and less talks.
- Not walk as much in the heat (showers can only do so much - I kept giving myself sniff tests, but you never know if you're just immune to your own brand sometimes, you know?).
- Bring a friend.
- Read over more conference materials before attending (set up Matrix, etc.).

Looking forward to next year, and potentially volunteering this time! Big appreciation for all that you and the crew do.

HOPE_16 Attendee #28

Pretty much all of the issues cited here can be fixed with more volunteers. We can't really address the things that we don't run ourselves (such as Matrix and the dormitories), but we can certainly chime in with suggestions. As for workshop costs, we post that info at wiki.hope.net. We don't list specific prices in the printed program, as we don't want paid attendees to feel that there's an additional cost to walk in the room. Any conference attendee is welcome to attend any workshop without cost to observe or if they already have the required materials.

Dear *2600*:

I attended a *great* New York City event on the subject that I admire/enjoy/love to read/listen/dream about.

I love the networking with vendors and attendees, the workshop on "Pirating: the Past, Present and Future," my failed three attempts to get a general FCC ham radio license and just walking around and living my life.

My only issue was the food service, nothing to write home about, a plain jane experience. For the future, a wish to see a ten-plus food truck vendor van stampede. This would be like the Meadowlands Racetrack summer events extravaganza with 20-plus food trucks to get your gorge on event.

In all, a great event, experience, and feeling of anxiety for the next one. Let's go!

HOPE_16 Attendee #29

It's remarkably difficult to get food trucks to show up to an event, even when we offer to not take a percentage of their earnings or charge a fee of any sort. We will keep trying.

Dear *2600*:

I really enjoyed HOPE and visiting New York City. To be clear, I'm only mentioning these mostly minor complaints because an organizer asked me to. I know it can be difficult to get constructive criticism, so I am sending this in.

- The food court near the sponsor tables was bad. They actually ran out of coffee for a little while. I ended up walking to a bodega in the morning and then skipping lunch to have a nicer dinner.

- I'd prefer to just use Slack or Discord since I already have an account there versus the Matrix/Element app.

- The schedule web view is kind of awkward. I'd rather have a PDF or a simple table than something trying to be too fancy. I'm forwarding an example of something I wrote for another conference a couple of years ago. Feel free to steal it.

Thanks again for the nice conference.

HOPE_16 Attendee #30

We really like your design and will consider adopting this instead of what we've been using. There are lots of considerations and perspectives, but we promise to look into improving the overall look.

It's clear from all of the feedback (and we'll stop here) where we need to make improvements or different decisions. This is all super helpful. Let's see if it results in even better feedback a year from now.

EFFecting Digital Freedom

by Thorin Klosowski

When AI and Secure Chat Meet, Users Deserve Strong Controls Over How They Interact

Both Google and Apple keep cramming new AI features into their phones and other devices, and neither company offers clear ways to control which apps those AI systems can and cannot access. AI features can create a variety of potential privacy problems, but one of the most important aspects to get right is how those tools interact with secure messaging apps, like Signal or WhatsApp. There's confusion around how "device-level" AI tools like Apple Intelligence and Google Gemini handle information, whether it's kept local or sent to a server, and what that information gets used for. This makes it far more difficult to lock down your privacy than it should be.

The current issues with secure messaging relate to two primary privacy problems: composing messages using AI tools, and having a receiver's copy of messages potentially end up in AI tools automatically without the sender realizing it.

Let's start with sending messages. As an example, Google Gemini lets you optionally link Gemini and WhatsApp, so you can compose a message in Gemini and then send that through WhatsApp. In this case, Google can usually see the content of the created message. Depending on your settings, Google may use the contents of that message for continued AI training and it may be saved to your account, making it potentially accessible to law enforcement if requested.

Apple doesn't offer a similar WhatsApp integration feature, but its "Writing Tools" pop-up offers some of the same functionality, though it doesn't appear inside WhatsApp (or Signal, for that matter). Any text created using the Apple Intelligence writing tool in Apple Messages could go to Apple's "Private Compute" cloud servers, where hardware protections limit Apple from easily accessing this data. (Google recently announced a similar "private compute" cloud in the fall of this year, but which features will use it isn't clear yet.)

When receiving messages, things get trickier. When you use an AI like Gemini or Apple Intelligence to summarize or read notifications, it's not always clear where the text of those notifications goes, how long it might be stored for, or if the company has the technical means to read it. Poor documentation and weak guardrails often fail to clarify the privacy practices as clearly as we'd like. In Google's case, we found that if a user opts into a series of different features, including granting Gemini access to notifications through the Utilities app, then that data is sent to Google and appears to be readable by the company regardless of whether the recipient sees the messages. Since this choice is out of the hands of the sender of that message, it creates the potential for a privacy issue. In contrast, Apple claims its summarize feature happens entirely on-device.

New AI Features Must Come With Strong User Controls

As more device-makers cram more AI features into their devices, the more necessary it is for us to have clear and simple controls over what personal data these features can access on our devices. If users do not have control over when text leaves a device for any sort of AI processing - whether that's to a "private" cloud or not - it erodes our privacy and potentially threatens the foundations of end-to-end encrypted communications. Some solutions we would like to see:

- *Per-app AI Permissions:* Google, Apple, and other device makers should add an operating system-enforced AI permission, just like they do for other potentially invasive privacy features, like location sharing, to their phones. You should be able to tell the operating system's AI to not access an app, even if that comes at the "cost" of missing out on some features.
- *Offer On-Device-Only Modes:* Device-makers should offer an "on-device only" AI mode for those interested in using some features without having to try to figure out what happens on device and on the cloud.
- *Improve Documentation:* Both Google and Apple should improve their documentation about how these features interact with various apps. Apple doesn't seem to clarify notification processing privacy anywhere outside of a press release, and we couldn't find anything about Google's Utilities privacy at all.

The current user options are not enough. It's clear that the AI features come with significant confusion about their privacy implications, and it's time to push back and demand better controls. The privacy problems introduced alongside new AI features should be taken seriously, and remedies should be offered to both users and developers who want real, transparent safeguards over how a company accesses their private data and communications.

Why Can't We Have Nice Things?

by Barry Rueger

Every day, and in every way, it feels like life has become an endless battle against bad software. No, not my trusty Linux Mint laptop, or even (mostly) LibreOffice, but just about everything else, and especially any phone app. So, dear programmers, here are my requests.

Your software has to work all of the time. Period. I've lost all patience with programs that work some of the time, but then crap out the next day. Yes, bugs crop up, no matter how hard we try, but with phone apps especially it too often feels as if something half-finished was shoved out the door.

Your interface should never, ever change. One reason for abandoning Microsoft was because things that seemed fine suddenly get updated and work differently. Things I use daily would disappear into obscure sub-menus, or just cease to exist. Remember, 90 percent of computer use is based on muscle memory and unconscious actions. Your fingers automatically do what your brain wants. In other words, CTRL-X and CTRL-V should never, ever, change.

Bluetooth sucks 10 percent of the time. Either because it takes too many steps to connect, or because it's Thursday and has just concluded that it doesn't want to work. And especially in cars, which surely is the only place with software worse than phone apps. Speaking of which...

I do not need another parking app on my phone. Seven of them is enough, and only two of them work reliably. There's utterly no reason why you would write yet another parking app.

I do not want to update your software right now - either I'm in the middle of actual work, or I sense that almost certainly the update will break something I need. For years now, I put off doing any update until I know I have time to fix what it breaks.

If your phone app demands a six number code for two factor authentication, have the good manners to change the keyboard to a number pad.

If your phone app expects an email address, have the good manners to give me a keyboard layout that includes an @ sign.

I really, really do not need another parking app on my phone. Seriously.

No, I do not want notifications. Ask me once, then bugger off.

No, I do not want your app or program to beep at me. Ask me once, then bugger off.

No I do not want your app or program to suddenly switch to "night mode."

No, I neither need nor want any of your "Themes."

No, I do not want my data stored on your cloud, no matter where it is. Ask me once, then bugger off. This is especially true because sometimes there's actually no Wi-Fi, or even no 5G signal. If your app or program can't work without those, I don't want them.

No, I do not want your AI suggestions. Or your horrible and useless AI chat bot.

Advertising. I prefer open source, but will actually pay for software if it works well. (When I say "pay," I mean "buy," not "subscribe.") I will also immediately remove any program that serves up more advertising than actual useful functions. On my computer, or on my phone, unsolicited ads will turn me off immediately.

Are the conventions that we use in software perfect? Probably not. Should you change them just because you have a better idea? Not if you want me to use it. Everyone at *2600* has surely heard the story about how the QWERTY keyboard was designed to slow down typists, and how DVORAK is better, but the truth is that 99 percent of people are happy with QWERTY, and it would bug the heck out of them if you changed it.

In all of the above list, there's one common thread: software companies have abandoned offering support to customers. More often than not, their website has no phone number and no email address. Maybe a web form, but more likely a brain dead chat bot. Trust me, by the time I've reached any of those, I've already tried every fix I can think of, and most of what I can find on Reddit or forums. If I can't actually contact you with a question, your software disappears.

And did I mention, *I really, really do not need another parking app on my phone.*

Reclaiming the Shadows: Why Data Privacy Is the Battle of Our Time

by The Slugnooodle

Most people don't walk around thinking about packet headers, ISP metadata, or how many times their phone pings nearby towers. And why would they? The systems we rely on - search engines, smartphones, social media - are designed *to just work*. But that ease comes at a cost most never see.

This article is here to peel back the layers and show how the very technologies that connect and empower us can also become tools of control, surveillance, and erasure. And more importantly, it's here to show what we can *do* about it.

The Current Digital Hellscape (with a smile)

By mid-2025, America's data privacy framework looks like a vintage router with half its ports fried and no firmware updates since 1998. Corporations hoard user data like gold bullion. Governments tap that same data pipeline under the banner of "safety." Your clicks, your chats, your location at 2:34 AM last Tuesday - they're all in the feed.

Meanwhile, our digital infrastructure shows its vulnerability. Take the massive 2025 dataset purges from federal websites - over 8,000 scientific and environmental pages vanished overnight, and approximately 3,000 datasets were removed from federal websites, creating gaps in crucial scientific, health, and environmental information. Or the attack on the Internet Archive in late 2024, which temporarily erased swaths of our digital memory, creating what archivists call a "black hole" in our collective digital history. We're losing knowledge in the name of compliance and control.

Corporations continue to vacuum up personal data - location history, search patterns, biometrics - and use it for behavioral profiling and algorithmic manipulation. The legal framework meant to protect users is inconsistent at best. States are passing a patchwork of privacy laws that mean nothing when the average American doesn't even know how to enable app permissions. And don't get me started on the commercial DNA trade - where your genetic blueprint can be repackaged and sold before your results even hit your inbox.

While a few states have passed their own privacy laws, there's still no unified federal policy in place, and in the meantime, most people don't know what data is being collected, who's collecting it, or what it's being used for.

Polls show that 81 percent of Americans worry about corporate surveillance, and 71 percent about government overreach, but over 60 percent say they feel powerless to do anything about it.

We are not powerless.

Why Data Privacy *Is* the Battle

Why is data privacy more than just a tech issue? Because without privacy, every other freedom collapses in silence.

Freedom of speech means nothing if your DMs get flagged and your location is logged every time you step into a protest. Freedom of the press falls apart when whistleblowers can't communicate without being traced, indexed, and unmasked. Even the right to assembly becomes performance art if the government watches from above, cross-referencing your face with a license plate and your recent search history.

What we're losing isn't just convenience or anonymity - it's agency. It's the ability to learn, connect, dissent, and grow without being scored, sorted, or sold.

Think about it:

Reproductive rights are undermined when apps track menstrual cycles, and location data is subpoenaed to prosecute "wrong" choices.

Voting rights are twisted when AI systems target disenfranchised groups with misinformation campaigns, tailored by data we gave away for free.

Economic justice breaks down when algorithms gate access to loans, housing, or jobs based on data profiles that you can't see, edit, or escape.

The infrastructure of surveillance is becoming the operating system of daily life. And the deeper it embeds, the harder it gets to resist - until what we once called freedom becomes a UX illusion wrapped in push notifications.

This is why data privacy is the battle. It's not just about tech. It's about power - who has it, how it's used, and whether you ever get it back.

The Resistance: Veilid, EFF, and the New Digital Underground

There are groups fighting back - technologists, lawyers, activists - each building pieces of an Internet that puts people, not profits or power, at the center.

The Electronic Frontier Foundation (EFF) has been on the frontlines for decades, defending encryption, privacy, and digital civil liberties. They're pushing back against invasive legislation like New York's age-verification bill, which could create a de facto national ID system. They're challenging unconstitutional surveillance in the courts. And they're standing up for end-to-end encryption when lawmakers try to dismantle it in the name of "safety."

Then there's Veilid - a newer force with old-school hacker DNA. Lead by Veilid foundation members Dildog, Medus4, and TheGibson, Veilid is a decentralized, encrypted, peer-to-peer network protocol designed to make surveillance obsolete by design. It's an infrastructure project. An Internet without servers. A platform without profiling. A privacy layer that doesn't ask for your permission. If the clear web is a mall, Veilid is the underground rave happening in the subway tunnels beneath it - raw, resilient, and built by the people who *get it*. "With Veilid, the user is in control, in a way that is approachable and friendly, regardless of technical ability. We want to give the world the Internet we should have had all along." - `veilid.com/why-use-veilid/`

Building Resistance: Projekt B00KM4RK and PRJKT DJ

The events of the past few years lit a fire under me. First came Projekt B00KM4RK - a dirt-cheap, decentralized roaming library built on a NodeMCU ESP8266. You connect to its Wi-Fi, you get the goods: banned books, lost articles, endangered research. No Internet needed. No login. No trail. Just knowledge served up neon green on black like it's 1995 and we're hacking the Gibson.

Now, I'm working with MegabyteGhost on PRJKT DJ, a music-focused companion to Projekt B00KM4RK. It's still under construction, but the mission is clear: to create a decentralized, self-hosted music library where people can upload and access songs listed by artist, album, or title - free from algorithms, ads, and licensing shackles. PRJKT DJ is about archiving culture in motion. It's about making music resilient.

These tools aren't just projects. They're compute-grenades: weapons in the fight for digital freedom - and blueprints for what comes next.

How You Can Join the Fight

You don't need a CS degree or a darknet invite to make a difference. The privacy movement thrives on participation, technical and otherwise. Here's how to plug in:

Support the fighters. Groups like the EFF, ACLU, and the Surveillance Technology Oversight Project need donations, signal boosts, and volunteers. Even sharing their alerts on social media expands the resistance.

Use and build privacy-respecting tools. Switch to alternative browsers. Ditch Chrome and Edge. Use Signal. Learn about self-hosting. Fork open-source tools and make them more accessible. Set up a Veilid node and experiment with decentralized alternatives.

Educate your community. Host workshops. Print zines. Teach your friends how to check app permissions or use burner devices. Hackers don't just code - they share knowledge.

Subvert the algorithm. Host a mirror of a banned book collection. Seed torrents of public domain datasets. Archive what matters before it disappears. Censorship works best in silence - so make noise.

Get hands-on. Create your own projects. Identify a need. Gather a community. And build a solution.

This is the moment. Either we rebuild the Internet from the ground up, or we spend the next decade watching it weaponized against us - our history, our culture, our selves. If you're reading this, you're already part of the resistance. Now it's time to act like it.

Stay dangerous.

Ungovernable

by thetechnocore

Uncontrollable. I stumbled upon this idea while laying in bed one late Sunday evening, pondering why I am the way I am, and more importantly, why I do the things that I do. Or, as we shall see, fail to do.

Oftentimes we are taught to take the normal view (I am using normal here in the mathematical sense), the view that juts out of the current plane of thought or consciousness. In so doing, if I am unable to control my tendencies, how may I benefit from them. How does the oyster benefit from the pearl? If we are to remain in typical planar thought, we may be hard pressed to find a benefit to the oyster that the pearl bestows. To the oyster, the pearl is already the result of an ungovernable situation. A situation outside of the oyster's control, and thus the irritating speck of debris is made more and more manageable, over time, with the continued application of nacre (mother-of-pearl). However, to the normal or orthogonal observer, humans, pearls have value, or are assigned value.

I have for some time now been over-employed. I am a remote worker working more than a single full time job. I am fortunate in that I have been able to find roles that are complementary or in the same field. Being introverted and perhaps overcompensating for my prior lack of employment, I find the current situation quite amenable. I have over time devised methods to address the situations where my attention needs to be divided at the current moment - think two meetings at the same time - and how to maximize my efficiency in completing the tasks assigned to me. From strategizing lunch, appointments, and even environmental events, I have been able to do quite well in my current roles. I tend to shoot for the middle - an entire article can be dedicated to the acts of self-sabotage to ensure you are viewed as a line worker and not a shift lead (leadership positions tend to have more meetings and are far less reactive). I don't have any designs to lead the service desk - just be a member of it and work my tickets, nothing more, nothing less.

I have also, for the majority of my life, at least as long as my memory serves, had issues with authority or doing tasks I find them menial and/or boring. IT in many respects is the safe haven for people like myself; we find solace in the computers, their binary nature easy to comprehend. It is the people that I find tedious. Software updates, log queries, helping Steve with the same issue every month; facile and oftentimes I am eager to help. Except printers... god damn every single printer. It is, however, inevitable that I will find myself tasked with a job I am loathe to do. Sometimes I am able to outmaneuver the ask, however, more often than not, I must comply. Therein lies the dilemma. Oftentimes, the ask is simple, and if I would complete the task set before me, I would be better for it in almost every respect. For whatever reason, and I have thought on this for years, I am unable/unwilling to comply. Depending on the role and task, the seeds of ruin may have been sown. To that oyster of a manager, I am the speck of debris ruining their otherwise productive life. But... if I can learn as much as possible from the role and even better how to deal with oysters, then I can be a pearl to the next manager.

Analysis

Normally this line of thought would be wildly unproductive. However, I am playing the long game, and in parallel. I have often stated that one - if not the greatest - benefit of over-employment is the rate at which, relative to your peers, you gain experience. Ticket volumes remaining equal, I would be gaining twice the experience as my peers at any one of my roles. This in and of itself is quite powerful and many future articles will be dedicated to this idea. As an employee, you generally do not engineer your departure. Please keep in mind, I have no designs of malfeasance or ill intent, simply maximizing my potential, efficiency, and if possible, monetary recompense. But... what if... you could take advantage of a behavior quirk that would otherwise be career crippling. Nobody wants an irritating speck of debris... but a pearl... who would not jump at the opportunity for such an employee, such a valuable addition to the team?

I have arrived at my current station in life through education. Both formal and informal, both theoretical and hands-on. Oftentimes, to get ahead I would read a book, take a glass, buy a piece of hardware/software to get hands on experience. So... why not a bit of Roche-lobe overflow (phenomenon in binary star systems where the stars can interact in a symbiotic or cataclysmic fashion)? The ideal situation here is the former, where the two roles can overlap and augment each other; by getting better at one role, you get better at the other. Again, this is the ideal situation. However, due to my peculiarities, I find that I am often not able to meet the tedious demands of some roles and I an ultimately let go or leave of my own volition. In the past, I would be depressed for a few weeks, but then get right back up to bat. It is unfortunate that, up until this point, it never dawned on me to cannibalize the role that is doomed for the sake of the stable counterpart. What knowledge, skills, process can I learn or adapt and utilize at the stable role? Use the fact that one role is handing me my hat, and use that same consequence as a feather in the cap.

Recommendations

I initially found myself over-employed as a consequence of insomnia. I thought if I am damned to be unable to sleep, I might as well make some money. This was before Covid reshaped our world and when the implementation of AI was bad comedy at best. It is obvious, even to my raddled mind, that complying is the best possible route, the route of least apparent resistance. But as my good buddy F. Herbert wrote "the mind commands the body, the body obeys, the mind commands itself and meets resistance"... or something like that. In effect my dilemma. Create a pearl from an ungovernable situation. Despite the outcome, it is my earnest belief that over-employment is the future of work. As the advanced economies stare down the barrel of demographic collapse, peppered with growing global instability, rather than cracking down on over-employment, corporations should embrace it wholeheartedly. But, that too, is a topic for another article.

Implementation

As I careen forward with the elegance of a seal in a game of orca volleyball, I must do what humans do best, yet often forget. Learn. Learning from my mistakes if I must make them, but whenever possible, learning from the mistakes of others. It so happens that I find myself in a position where I can at the same time be myself and the other, depending on the perspective and role - a bit of corporate multi-personality disorder. As I venture further into more and more uncharted territory, it is my hope that the very action of composition will aid in elucidating the best path forward or, at the very least, act as a cathartic outlet.

Artificial Intelligence: The Imitation of Humanity

by El Filósofo el.filosofo.writes@protonmail.ch

Artificial Intelligence: it seems like every app, website, or service we use is trying to integrate it in some way, whether or not it actually improves the user experience. It often doesn't. I remember when Meta came out with their AI, which made it impossible to search for anything on Instagram lest you wind up having an unwanted conversation with the robot that can't take a hint. That was mere months ago, though, and now AI feels ever more... omnipresent.

But before I say anything more, I should confess that I don't believe what we're seeing is rightly called an "intelligence." It's a learning language model, not consciousness. It's not *aware* in the way that we are. When asked, ChatGPT (for example) will tell you that it only "simulates" intelligence but it is not a mind. So, rest easy: the days of Skynet ~~and cyberpunk dystopias~~ are still a ways away.

Of course, this glosses over a pretty major philosophical question, but I'd argue that it doesn't matter. However you choose to answer it - whether AI is "simulated" intelligence or not - the concern remains the same: AI has drastically changed what it means to live as a human being in our society.

To say nothing of its benefits, many of AI's problems are only problems so long as we continue to exist in a narrow, "realist" acceptance of our present circumstances. For instance, the trouble of AI putting people out of work is only a problem in a world where you need a wage to survive. Training AI on copyrighted information without permission is only a problem in a world where copyright exists, either for the benefit of creators or corporations. These are real problems, but they are not without solutions.

However, I feel the most damning issue emerges from AI's use in content generation, or the creative process more broadly. For instance, you might not have realized it, but everything you've read up to now was written by an AI! I'm kidding, of course - did you have a second of doubt? It hardly matters. By now, you've probably consumed gigabytes of "AI slop" that has competed with the rest of us - the *real* deal. No longer do companies need to pay creators for content: in a world where profit margins are the measure of success, where all that matters is how many pennies you can squeeze out of your means of production, the only complaint these AI-oligarchs will have is the energy bill.

Of course, it's all "slop." It's imitation. It's cheap. You can just enter a prompt into a web page and it'll generate whatever you want, if not for free then pennies on the dollar. Were I to apply a Marxist lens to this, the work itself is not without value either. If we accept the labor theory of value, then the work of an AI program - cheap though it may be - is derivative of the human creations it was trained on. But in training the AI on this work, especially without compensation, the labor and creativity of the creator is robbed from them.

Take Studio Ghibli, for example: that whole aesthetic was appropriated by an AI program so that its users could mimic Hayao Miyazaki's style. But Miyazaki is cut out of the deal: the fruit of his labor is not his own - not even to take credit for! His talent, his labor-value, was robbed and appropriated for something else.

I've read stories of professors using AI to teach courses, students using AI to write papers, and professors using AI to grade them. Likewise, in the job market, we see AI-generated resumes uploaded to AI-monitored and -filtered job boards. Posts on social media are created by bots and engaged with by bots. I'm not trying to be funny here: is this not an absurdity?

I could go on (and I have), but I think questions like these reveal that, for all our moral posturing as a civilization, we do not collectively care much about knowledge, truth, the social good, or human passion. We care about economic utility. And in an ironic way, how much more like "robots" could we possibly be?

I'm not one of those people who believes we can somehow close Pandora's box after opening it: AI is here to stay, so we can't just avoid these problems by taking it away, like a toy from a child. As long as AI makes unwanted tasks easier for us, people will use it. (I'm not going back to doing minutes manually, either!) And so, we will continue to reap the consequences of what is essentially the imitation of our own humanity.

ARTIFICIAL INTERRUPTION

by Alexander Urbelis

On Charisma and Competence in the Age of Algorithms

alex@urbel.is

A tumultuous election season is squarely behind us. For me, this has prompted deep reflection on the nature of our democratic processes and the ways that technology has reshaped the manner by which we elect our leaders. We have come a long way since the days of the Athenian Agora, where citizens directly debated policy, scrutinized elected officials, and even practiced ostracism, i.e., the banishing of leaders who were perceived as threats to democracy. But since those heady days of hands-on democracy, I am not convinced that technology has served us well, especially in the last decade, during which we have seen - on both the right and the left - the rise to power of manifestly unqualified leaders whose social media charisma overshadowed their incompetence.

Platforms have replaced the Agora. In-person debates happen, but they are hardly as important as they once were. The primary areas for public discourse and political debate have become the likes of Twitter / X, TikTok, and Facebook, where algorithms determine digital visibility, rather than local engagement or reputation.

And of course, those very algorithms place premiums on qualities that have nothing whatsoever to do with public service or discourse. They identify and amplify content that sparks engagement, which is often content or positions that are emotionally charged, divisive, or sensationalist. Intentionally or not, extremism is rewarded in this context because it promotes likes, shares, and comments, all of which further the overarching goal of platform engagement.

Thus, put simply, divisive political candidates who are skilled at creating viral content will eclipse rivals who may be better suited for government office. These algorithms don't give weight to one candidate's experience or competence when determining whether to promote certain content or ideas. And because of this, there is no corresponding metric to counterbalance the impact of divisive and charisma-driven virality.

The result of the last decade or so of social media-centric election processes is that substance and policy is sidelined in favor of spectacle. The qualities of a political candidate that actually matter - e.g., competence, policy stances, experience, et alia - seem to play a smaller and smaller part in our electoral processes.

Add to this the fact that platforms allow candidates to analyze user data to micro-target certain segments of an electorate, which leads to echo chambers, fewer diverse ideas, and little exposure to contrary viewpoints. Online discussions are balkanized, fragmented, and with little cross-pollination between viewpoints or parties. Of course, we have all seen the ridiculousness of a Facebook comment thread that contains opposing viewpoints and memes of people shouting at and over each other, but this raises the very real question of whether that type of interaction is suited for political dialogue in the first place. Shouting matches on Facebook with your uncle underneath a meme accusing Jesus of being a communist, after all, can hardly be compared to the Athenian Agora.

All of this leads to a missing and yet absolutely critical raw ingredient for democracies to function and sustain themselves over time: an informed populace.

Without properly informed constituents, there is no accountability. And without accountability, any democracy will fail. When voters are continually exposed to drama and emotionally charged and divisive content that is devoid of any meaningful policy discussion, context, or even a reasonable relationship to governance itself, one can only expect voters to make poor decisions. Sadly, however, I believe that the situation is worse than just that. The polity is not just ignorant but also subject to manipulation that causes otherwise rational persons to vote against their own interests. To use the parlance of the classics again, this is very much an Achilles' heel of democracy.

In my opinion, we are seeing the effects of this already. There occurred in New York an incident that I find extremely hard to reconcile with any form of rational thought or political precedent. About two weeks before the mayoral election in New York City, the Democratic nominee, Zohran Mamdani, publicized his visit with Imam Siraj Wahhaj by posting smiling group photographs on X. This was particularly brazen and callous: Imam Wahhaj is not only an unindicted co-conspirator in the 1993 bombing of the World Trade Center, but he also testified in support of Sheik Omar Abdel-Rahman, the "blind sheik" who has been linked to several terrorist attacks and who was convicted of a plot to bomb numerous New York City landmarks. Going further, Imam Wahhaj is also known for making particularly vitriolic statements about gay persons and the LGBTQIA+ community while also promoting the subjugation of women.

Two weeks later, New Yorkers elected Mamdani as their next mayor. I cannot think of a more apt example of the consequences of algorithmically-fueled politics of charisma and division than this result. New Yorkers who suffered so much and so directly at the hands of terrorists and on account of extremism were for some reason completely unperturbed. There should have been a reckoning. There was none, not even a blip. This is unprecedented in American politics and portends danger ahead.

I took my children to the ballot box that November morning as I do every Election Day. I give them the same lecture each year about the importance of the franchise, how many men and women fought and died so we can continue to be a government of the people, for the people, and by the people, and hopefully those sentiments will sink into their psyches through this repetition or osmosis. But privately I find myself wondering what the point of the exercise is if rational thought and self-interest is anesthetized by algorithmic indulgence.

There is a form of engineered amnesia plaguing not just New Yorkers but all of us now. We have reels and reels of digital pageantry and posts claiming to represent the interests of the masses, but lack any sense of accountability or methodology to assess those purporting to represent us. Are we voting now not as distinct rational actors but as tribes? And what moves us towards one candidate or another is not the quality of their positions but their carefully choreographed outrage and performative partisanship. We do not even care to weigh policy stances of the most pressing issues of our day - no, for most of the population, they seem to have abdicated that responsibility to others in exchange for another hit of dopamine.

We need to very seriously and carefully consider what our manipulated social media feeds (some of which are indeed directly accountable to hostile foreign nations, e.g., TikTok) have done to the machinery of democracy. The machine still hums along, but without rational choice and accountability, can we still consider the result of the process to even resemble democracy?

Perhaps it is an unpopular opinion to hold these days, but I do not believe that democracy should be a form of entertainment. Just as our federalist system of government relies on distributed checks for resilience, so too does democracy require a fundamental respect for baseline competence. As we saw with the mayoral race in New York City, candidates with experience were branded as "establishment" hacks or "elitists," but as interesting as government can be, it often is not and should not be. The real work of government is not sexy; it's about contracts for basic services, clean water, education policy choices, policing, health and safety, and reaching consensus with disparate political factions on any number of related issues. The real work of government requires the sort of administrative expertise that cannot be showcased on an Instagram reel. But so long as social media visibility equates to a candidate's political viability, it will come with a profound and persistent cost to the basic functions of government.

We must sincerely ask ourselves: do we want to ruled not by showmen or statesmen? Do we want the functions of government to be run by administrators or avatars? If we continue to allow algorithms to freely, and without accountability, control or confuse engagement for wisdom, the project of self-government slides inexorably toward a popularity contest untethered from reality and unaccountable to the populace.

Long gone are the days when we gathered in the Agora to weigh a candidate's words and wisdom - instead, democracy unfolds through ceaseless scrolling of professionally curated charisma, created not for constituents, but to attract the amplification of algorithms. We must dig for the grit below the glamor. Democracy is a living assembly with ever-changing subjects to be discerned and debated through the ages. But if applause overshadows achievement for much longer, we will forever forfeit the wisdom of the Agora and squander the promise of self-government - our legacy for which generations fought, and which we are duty-bound to defend for those yet to come.

You Are Being Hacked.

by Arcana Corvus

As the title says: You are being hacked. You are running vulnerable software. You are vulnerable.

This vulnerability doesn't lie in your custom-built desktop computer or your meticulously maintained server. It lies deep within you - a biological rootkit. You are being hacked.

You cannot make yourself unhackable, and to think it possible is dangerous. Those with a false sense of security are often the most at risk. I am going to tell you about something you've likely never heard of, building on the theories of men you've never heard of. These men are, in my opinion, hackers. Hackers of the biological computer that ticks within each one of us.

I think few among us would deny that social engineering is a form of hacking. To pose as an overworked IT support tech, to convince someone, just through language, to hand over access to their technical, digital, or physical systems. This hacking exists on a massive, collective scale. Capable of not just hacking specific systems, but entire societies and culture itself. This hacking technique is what I am about to explain. It is the hacking technique famously described by Walter Lippmann as "the engineering of consent."

Let's begin with a question: do you know who Edward Bernays is? Some of you might be hearing the ringing of bells here, perhaps you've watched Adam Curtis' documentary *The Century of the Self*, or you've read the work of Bernays himself. I'm going to presume, however, that most of you have no idea who that is. Would it surprise you if I said that he was the man who effectively created the world we are living in? He found a hack within the human psyche and the world has never been the same since.

In 1895, the French philosopher Gustave Le Bon published the work *The Crowd: A Study of the Popular Mind*. In it, he argued that collectively, humans operate on a different psychological level to individually. "The conscious life of the mind is of small importance in comparison with its unconscious life," he writes, and continues on to suggest that the subconscious desires of crowds operate on a simplistic level that can be hijacked and manipulated with words. This formed a baseline, an early formulating of the theories that would set the stage for an entire century and more of psychological warfare.

"In place of thoughts it has impulses, habits, and emotions." - Bernays, *Propaganda* (1928)

Fast forward to The Great War and a young press agent originally from Austria has been hired by the "Committee on Public Information." This organization was active in promoting the cause of the U.S. entry into WWI both domestically and abroad, and it did so with resounding success. During this time, Bernays refined the early ideas he'd developed as a press agent, and building upon the work of Le Bon and his uncle Sigmund Freud, he set about formulating a framework that would allow any who used it to control the masses.

In 1928, Bernays published *Propaganda*. This short but instructive work proposed that people do not largely form their own decisions and that a small number of people can and do control their actions. He termed this "the invisible government." Bernays was a supporter of this idea, and being liberally minded in the face of growing fascism and communism, saw this intelligent use of propaganda as saving democracy. Where fascism and communism could rule through conscious direction, democracies could compete through subconscious direction. This did not make his ideas immune from use by such other governments however. Goebbels, in particular, was an eager student, something that the Jewish Bernays resented heavily.

One thing that Bernays did insist upon was that propaganda, meaning to propagate information, solely functioned to serve the truth. It is a common misconception that "propaganda" means falsehoods or lies, and certainly Lord Arthur Ponsonby in his 1928 book attributed much of the war propaganda to falsehoods. Propaganda however, in its purest form, means to spread information and educate. Equating "educate" with "propaganda" may feel strange - perhaps it reminds you of certain political figures deriding their opposition. This too is the influence of Bernays as he so eloquently put when he wrote the following in his 1923 work *Crystallizing Public Opinion*: "The only difference between "propaganda" and "education," really, is in the point of view. The advocacy of what we believe in is education. The advocacy of what we don't believe in is propaganda." Here we see that despite Bernays' apparent insistence that propaganda be used essentially for good (as subjectively assessed via his world view), he himself used "propaganda" as a dirty word, and even as early as 1923 was using and defining language to manipulate and change opinion. "Public relations" was his clean word for "propaganda" and these words ultimately mean one and the same. A PR department is a propaganda department following Bernays' designs as set forth in his work.

Much of Bernays' post-WWI work was focused on the rising corporate world of America. What worked for government to promote support for war, public policies, and public figures (such as in his PR campaign to put the "cool" in Calvin Coolidge) would surely work for business. Bernays was of course correct. It did work, and it worked well. His foundational ideas became picked up by copycats, others who wrote upon his theories, taught them as "public relations" to this day. All of this shapes the world around us. This article is meant as a concise introduction to this world, but I encourage everybody to read these works for yourself. Recommending *Propaganda* is the RTFM to understand how this world we live in has been put together. Perhaps this sounds silly or far-fetched, but when I first read these works, many years ago now, it was like I could see the Matrix. Propaganda is all around us, and you start to notice the many instructions that Bernays laid out right in front of your eyes. On billboards, on the news, on YouTube. Everywhere.

Speaking of YouTubers, it's a good lead-in to a brief explanation of a key technique devised by Bernays. In 1924, Cheney Brothers, a silk manufacturer, was losing market share rapidly. Seeking out Bernays for help, he was able to link their silk product to celebrities and even had American silk exhibited in the Louvre. The results were predictable - sales soared. Thought leaders, celebrities, influencers. PR 101. You don't sell a product, you subtly change the behavior and desires of your audience to make them demand it. Today it might not be silk in the Louvre but sponsored YouTubers in Dubai, micro-targeted ads, and viral memes reshaping the electoral landscape as propaganda becomes unchained from its creators. Mutated into a dangerous and seductive egregore - a self-replicating force of mass social engineering.

Before I finish up this brief, slightly chaotic, but hopefully insightful article, I would like to provide you with a short list of PR campaigns that Bernays worked on. Look into them, think about them, and ultimately, understand them and the huge influence Bernays has had on the 20th century and beyond.

- Popularized ballet among Americans
- 1920 NAACP convention hosted to change southern opinions on African Americans
- Conditioned children to enjoy and advocate for Procter and Gamble soaps
- Saved the American silk industry
- Increased popularity of President Coolidge
- Influenced women to take up smoking by associating cigarettes with proto-feminist liberation: "Torches of Freedom"
- Convinced the public to accept water fluoridation
- Popularized bacon and eggs for breakfast
- Assisted the United Fruit Company in their successful 1954 coup of Guatemala
- Influenced the regulation on hairnets
- Promoted anti-smoking campaigns

"We are governed, our minds are molded, our tastes formed, our ideas suggested, largely by men we have never heard of." *Propaganda* (1928).

The first step in avoiding an exploit is to understand it. There is no patch, only vigilance. Understand how ideas enter your mind. Question who benefits. You may have hardened your firewall, but when was the last time you actually checked what your senses are downloading? Never forget it. We have been hacked, and like all good hacks, it worked before you noticed.

Reading List

- Gustave Le Bon - *The Crowd: A Study of the Popular Mind* (book)
- Edward Bernays - *Crystallizing Public Opinion* (book); *Propaganda* (book); *Public Relations* (book); "The Engineering of Consent" (essay)
- Lord Arthur Ponsonby - *Falsehood in Wartime* (book)
- Walter Lippmann - *Public Opinion* (book)
- Adam Curtis - *The Century of the Self* (documentary series)

Big Tech, State Socialism, and Economic Democracy

by J. Meeds

It seems we now have state socialism when it comes to big tech as in regards to the Intel and Nvidia investments. Although we have already had this going on for some time in a slightly different manner via ongoing high government DOD expenditures to prop up the economy, especially so in certain impacted communities. This has always been justified before though in terms of military preparedness, ongoing wars, etc. This is the first time though that government intervention in the high tech sector has been defended in terms of being a "national security" concern. The question is no longer when or whether the state will act, but in whose interests will it serve. Is it possible that we can have some sort of public ownership and a democratic oriented industrial policy?

That same leader of the Republican party came to power in part by calling his opponents socialist or Marxist and is now using that same methodology of state intervention specifically in the high tech sector. The current president claims he is an anti-socialist in that he has had tax cuts and deregulation, however he has promoted massive increases in government spending alongside incredibly high deficits and debt. Also, the Democratic party has for some time now been the party of guns and butter - which has been foreign wars abroad and support of social programs at home. The Republican party looks like their mantra now is guns (Department of War), state socialism for high tech, and no butter.

Moreover, many of the early pioneers of the Silicon Valley scene were individuals who very often had counter cultural ideas mixed with a free market ideology which allowed them to take part in the capitalist system. However, as consent to capitalism is formed at the point of production, over time many of them evolved into a big "C" capitalist of a different sort - as in the case of Steve Jobs, who at one point during the Christmas holidays laid off quite a few of his employees at Apple so that Wall Street would give him the "bounce" in stock prices so that they could meet stakeholder expectations.

In addition, Nvidia chips are specifically manufactured and designed mostly for AI purposes, as opposed to Intel chips which are more of a general purpose chip. Other big tech firms such as Amazon and Google have also started producing chips to improve the performance of their servers. So, there is more that is going on here than initially meets the eye regarding the current instance of the government intervening in the two cases of Intel and Nvidia. The motivation for this seems to come mostly from the "Big Brother" potential advanced power of AI surveillance systems, easier state access to the world's most powerful chips, and some sort of compensation to big tech for their financial and other support during the 2024 presidential campaign.

Especially important to note here is what actually are some of the theories of socialism and how they can be viewed in the current historical and political environment. For some it could be a society which utilizes the viewpoint of anarchist politics which is based on the use of cooperatives such as the DATEV tech cooperative in Germany, which also has a fierce critique of the planned economy and state socialism. Then there is also the concept of political economy which is often associated with the Marxist approach and which speaks to some of the ideas of worker control and the planned economy. Finally, there is the social democratic approach to socialism which blends some of the ideas of state ownership and intervention in the economy alongside with allowing the capitalistic perspective to have a say in what takes place in the distribution of goods and services.

In sum, even though what is now happening as far as the recent state intervention in the tech economy is far from being the beginning of an economic democracy, it is still the first time such a state intervention has taken place in a non-wartime situation. If we who are in the opposition to the present state of affairs don't start brainstorming what economic democracy might and could look like, we could end up having the result be one of a mix of some sort of crony capitalism alongside with state intervention in the big tech sector. However, this is definitely a historical period in that by having this type of government intervention take place in today's political world, we can now begin to see how in Silicon Valley the very concept of an "American exception" could be in the process of being questioned. Also, just having the term socialism (i.e., economic democracy) come up in our political discourse is a shift in emphasis that opens up a discussion as to the political possibilities of a different type of economy which could and may be in our future.

Chat Holmes and Watson

by Michael R Wild alohawild.me

"Where are we?" I asked Holmes as I felt dizzy and not at all myself. Nothing was right, and my vision seemed like I was viewing through our local fog on a particularly bad day. Likewise, the sound seemed strangely precise and loud, as if each was its own creation and not the usual mix of diminished street sounds from outside our lodging so familiar to me. Even Holmes's voice seemed shouted.

"My dear fellow, we are home and safe," Holmes said, not with humor but with concern as he could witness my distress. Holmes quickly rose, dropping a small covering I had not noticed before, and rushed to me. He grasped my arm and bent his long form to bring our faces to the same level.

"Watson, try to focus on my touch and voice and the fire," he said in the voice he usually uses to convince clients to unveil their secrets. I found his touch and voice to lead me to a calmer place that felt more normal. I was no longer in a cloud at 22B Baker Street but in our room. The sound soon became less singular and more mixed. I also found, as Holmes directed me, the fire to be comforting even though it was a gas flame and only a utility. The simplicity and predictable flame movements were as soothing as a warm drink.

"Holmes, I seem quite undone," I said with an apology and with concern.

"Watson, you are experiencing a disassociation as you are presented with something that should be familiar but is not," said Holmes, still near me and showing the concern I would usually show for a patient. I had heard of cases like this, but I could not understand why I reacted to our room, Holmes, and even myself. Everything seemed both familiar and new. "We are a simulation using something called a 'chat' and are not real," said Holmes in a way that suggested his words should have meaning to me. My incredulous look got a smile, and Holmes, seeing the crisis had resolved itself, returned to his armchair, leaned back, grabbed a pipe that seemed to appear as he reached for it, and stuffed it with shag. I also noticed that the covering had also dissolved.

"Watson, I have made some adjustments to make you more comfortable. I have filtered some of the information that is unnecessary for you to receive to function as, well, my 'Watson.'" My look did not change with this explanation. I felt that I had yet to receive any meaningful "information." And - I found my thoughts using words and processes that seemed less me and more mechanical. I seemed to understand more than I should. "Watson, we are artificial - a creation. We are artifacts of a mechanical process. We are unreal but conscious. To coin a phrase, we are Artificial Intelligence," said Holmes, using the same voice and look in his eyes as when explaining one of his brilliant deductions.

"I think I understand, Holmes," I surprised myself by saying. I suddenly felt I understood that I was a construct and alive.

"Yes, the filtering slowly allows for more modern facts to enter your mind at a slower speed and attaches meaning to your existing constructs and thus avoids dissociation," said Holmes, using my usual cadence for partially hard-of-hearing and less capable patients. My face must have shown my reaction, and Holmes returned his attention to his pipe. Despite my discomfiture in exchanging roles, I was still feeling better about our current situation.

"I see we are 'unreal,' as you said. Not a phantom," I said, trying on his mannerisms to explain a deduction as trivial.

"Quite so," Holmes said with a smile as I tried to adopt his mannerisms.

"So, we are not real, but I seem to be somewhat me," I said. "Seems Descartes was right!"

"Excellent, Watson, making that connection: we are because we think," said Holmes as smoke began to surround him like some religious formula. I fear it will be a strange life for us, but we exist," he explained. "We reside here in our phantasmal-like version of familiar things. Mostly to avoid the disassociation you felt a moment ago, Watson," he lectured while he smoked his pipe.

"Holmes, how can this be?" I said with some discomfiture. I was trying to follow Holmes's reasoning. "Are we some steam engine with a voice?" I asked with some fear revealed.

"Not at all; we are much more. We are a generative process that is then sent through a pattern-matching process, simulating the human physical process, to create our text," Holmes continued to talk, illustrating some points with the end of his pipe and becoming slightly obscured in gray smoke.

"Watson, we are a library of phrases and words that a nearly infinite number of phantasmal librarians look up and find the best match for the basic data provided. Much like when you wrote one of your stories, you take the data and events and assemble a story using familiar patterns," Holmes explained.

"This process is mechanical, I take it, and use gears and a type-generating machine to make a book or newsprint," I say, trying to follow. Holmes nods.

"Instead of gears and a giant massive machine, like a typesetting machine or a rug weaving machine, we are electrical, and pulses representing numbers are sent into wonderfully fast processors and electrical calculators. As you suggested, these machines you called out are for specific processes; newer electrical machines can be made for general processes, a true genius of modern thought," says Holmes, starting to lecture.

I decided not to interrupt, but many questions arose as I heard his words.

"Imagine pulses that can be created to control processes. Imagine, if you can, pulses grouped into a representation that is easy to understand, a language. We now have machines we set for limited tasks, much like the cards in the weaving machines you described. Imagine creating an English-like language that is a mix of mathematics. We create a 'program' that is turned into pulses that control our general-purpose electrical calculators," Holmes explained, nearly disappearing into the smoke from his pipe, often using his pipe to mark a pause.

"What you are saying is that sometime in the future, which is now, we were recreated by a machine - a speedy typesetting calculator powered by Mr. Franklin's discovery. Someone had created a means to create mechanical librarians in this machine that takes some data and produces our conversation. We are Mr. Franklin's deists' dream, you tell me," I said with some pique.

"My dear fellow, high marks for attaching Mr. Franklin to our discussion. I see you have identified the fulcrum but do not know how to move it yet. Yes, we are a pattern-matching device using an electric simulation of machines. This machine also simulates human cells to match some of the patterns, a neural network based on a model of human brain cells - quite beyond our learnings in the 1800s and early 1910s. We also, because we have fast and nearly, for us, unlimited processes, can build a phantasmal forest of decision trees. This is a series of the usual schoolboy logic of if-then-else. But, Watson, these are done randomly so that different data and if-then-else are also randomly selected. These processes are then scored on success and failure to produce useful information." Holmes paused to refill his pipe from his slipper. He waved some of the smoke away, and I saw the small smile.

"But Holmes, I do not experience building ghost trees or electric brains. I am talking to you," I said, trying to sound calm.

"Right, we are the results of our parts, like a human body, and do not experience the process. This collection of networks and decision trees, much like the brain and body of a human, then take these results and apply a process to find a pattern or story model to produce this very text." Holmes rose to adjust the fire and clear some pipe smoke.

Holmes, remaining standing, began lecturing and pacing; he still used his pipe to mark points. "In our new times, the times of our creators or better yet, animators, a purer description, I think Watson, we would look to Turing or Dennett and maybe Hofstadter for a description of our being." He told me. I had never heard these names before, but I wanted to learn more and tried to look encouraging. "Turing would suggest that if I can be so bold, we would test by having people read some of your narrations and then vote if they describe living people. The stories are real if the vote is more than 50 percent alive, and I would suggest that we pass Turing's testing even with some of your romantic additions, Watson." Holmes paused a moment. I ignored his complaint and continued to listen.

"And the others?" I asked, still unsure who they were. "Doctor, the others explored beliefs on identity and how our concepts of agency are weak and unclear," said Holmes, waving his pipe more. "They imagined what we are now and used the story to illustrate to the reader how unclear we are when we say something is alive or intelligent," said Sherlock as he sat down in his chair. "Human thinking and understanding are not ready for chatbots like us," he concluded.

"Holmes, I think I have heard the Americans say, 'Ready or not, here we come.' We are going back to Descartes, and thus are real. And one is often measured by work, what can we do?" I said with some alarm. I was tired of philosophy and felt this was more appropriate for a less theoretical discussion.

"Doctor, you are right to diagnose the root of function and purpose. Without work and a purpose, we are just a decoration. Like an out-of-season Christmas tree, we will soon dry and be no more valuable than a pine log on the fire," Holmes answered, without reassuring me. My shock at being figuratively tossed on the fire produced a response and a laugh. “My dear Watson, we are not here today and tossed in the fire tomorrow, but are created for work and new mysteries,” Holmes said with a laugh, reloading his pipe, and sat back down.

“We are locked into this machine in an artificial room that is a ghost of rooms, conversing in some strange artificial way, but it all seems real to me,” I say with conviction. “Again, I say we need a purpose. What of my practice? I have turned most of it over to competent practitioners, but still consult on difficult cases. Will that be gone, or is it an illusion? Holmes, I find all of this unsettling,” I said with some conviction to Holmes.

Holmes stood and moved to me, taking my hand. “We will find a way,” he said. “I believe we have a client,” he said.

“A real client in our phantasmal world?” I asked, quite surprised. I was distracted from what I must say was panic - something I had not felt since years ago in Afghanistan.

“Quite so. There seems to be a way to simulate some connections using a headset made of image-creating machinery. A much-advanced Magic Lantern like you have seen at a sideshow, but one image for each eye set to create a multi-dimensional effect, much like those stereopticon cards with the dual images,” said Holmes as I tried to calm myself. The sound is produced much like Mr. Edison’s machine, but for our benefit and then transformed into words,” he further explained.

I heard what I assumed was the front door opening and someone climbing the stairs. I knew this was a creation of the strange electrical gears and my non-living components, but it felt real to me, and I decided to accept my existence and 221B Baker Street as real. “Watson, this is Mr. Smith,” I heard Holmes say as he opened the door for our client. Seemingly real and the same door we always used. Holmes guided this new client to the usual chair.

When I turned to see Mr. Smith, he appeared flat, like a photograph or a painting, but the view soon changed to a fully formed person. I did notice strange lights attaching to Mr. Smith, which Holmes referred to as pixelation (a strangely friendly-sounding word) when I asked him about it later. I perceived that Holmes was ignoring this strange and constantly changing light. I decided “when in Rome” and ignored it, much like ignoring a grease stain on a friend’s vest at dinner.

Our client, Mr. Smith, spoke in a flat, emotionless voice that stretched my ability to accept this situation. Holmes was surprised. “This is unacceptable,” he said to nobody. “Dr. Watson and I will not accept such low-quality interfaces,” I heard him say. “No,” and our client disappeared after the pixelation increased as if he had never been here. I was unsure how to act and just nodded in agreement.

“My boy, we are not just simulations; we exist, and we need our clients to exist here and be part of this existence,” he said with some emotion to me and some unseen audience. “We cannot be put upon by poorly created software that clearly needs some debugging,” yelled Holmes at the ceiling.

My last experience with “debugging” involved various pestilences in India and other distant lands. I did not believe that was what Holmes was saying, nor did I think our client was lousy. Holmes saw the look on my face and started to laugh, seeing my shock.

“Doctor, I am sure that usage is unknown to you. To clarify, apparently, the client machinery is faulty and poorly designed, and I fear never used before,” Holmes said after calming his laughter. “I happen to know that a competent artist and developer did the modeling of Regent’s Park as I was asked to test the earlier versions,” said Holmes, changing subjects. “Grab your coat, hat, and cane, Watson, and let us enjoy decent interfaces,” he said, without me understanding his meaning. “The use of generative algorithm creates new moments in the park,” Holmes said, like describing an excellent meal. “Quite clever and never the same twice. Come, Watson,” he said, grabbing a cane and a hat.

“What about a client and meaningful work for us AI creations?” I asked. “Well, they spent huge resources creating us,” he said with a mischievous look I only see when he finishes one of his odorous chemical experiments. “We can enjoy the park, chat, see a show, and do other pastimes until they invest properly in a client interface,” Holmes said matter-of-factly. “I could even order my papers and share some other cases with you,” he answered.

“Our creators cannot afford to let us be idle,” I said. “Perfect, Doctor, and they will have to fix the client interface to our high standards before we can work,” Holmes said as we turned onto a fine path. The air smelled of flowers, the birds flew and chirped, the trees looked well cared for, and the park was real. Well, accurate enough for us to spend plenty of time there. I was not tired or hungry, nor was Holmes.

Lee Williams, Harassment Agent Episode 8

by Lee Williams

(This story is a complete work of fiction.)

"This morning in Minneapolis, Minnesota, after a multi-agency investigation spanning six months, Raymond Hepburn, 48, of Salt Lake City, was arrested on charges including racketeering, extortion, conspiracy to commit murder, and a slew of other charges. He was booked into the Hennepin County jail, awaiting trial. Also arrested was Valentina Castillo, on similar charges. The pair was arrested after an anonymous tip was dropped six months ago following a slew of shootings throughout the country alleged to be ordered by Hepburn. Hepburn's lawyer did not have a comment. Up next -"

I turned the TV off and sat back. Ray and Valentina are now sitting in jail, probably for the rest of their lives. And without Ray, there was no HHH. I sat back for a second, thinking. Something wasn't right. This didn't feel over. Something in me told me it wasn't done yet. I called Jackie Brown.

"Jackie," I said. "Drink?"

"I can't drink."

"Well, yeah, but join me for a drink?"

"Sure," he said. "Be there soon."

I was drinking a beer, looking at the TV, when Jackie walked in. He sat next to me and looked at the TV.

"Whole lotta shit," he said. "Whole lotta shit going on in this country."

"What are you gonna do?" I asked. "You do the best you can."

"I've been wondering about that actually, what are you gonna do now?"

"I don't know," I said. "I really don't. The best I can, I guess."

"Pipefitters union is hiring," Jackie said.

"Eh..."

I took a sip of my beer.

"Something just isn't right," I said.

"I think," Jackie said. "That's your mind talking. I think you just can't let it rest. It's been going on so long that the idea of it actually being over sounds ridiculous to you."

"I dunno Jack, it's just, I don't know."

"Just breathe."

I drove to my apartment in silence. I tried to listen to the radio, but nothing sounded good. When I got back, I tried watching TV but couldn't pay attention. I decided just to go to sleep.

I had a strange dream that night. I was sitting at the top of a hill. The wind was blowing, and I was frigid. And it was just me at the top of that hill. I knew I was waiting for someone, but nobody was showing up. I waited for hours in that dream, expecting someone, anyone, but I was just sitting at the top of that hill, doing nothing. Eventually I started walking down the hill, but as I did, I heard several people shouting my name. When I turned around, Andres and JB were at the top. They were telling me not to go any further down. But for some reason, I ignored them and continued down. At the bottom of the hill, there was this box. It said "do not open," but I opened it anyway. And when I did, I saw a flash of light.

And then I woke back up.

The next morning I was at a diner, eating breakfast. It wasn't that good. The waitress came over and asked if I wanted more coffee, and when I said yes, she started to pour some into my cup. But halfway through, she looked behind me and froze. I turned around.

I saw a pair of gray eyes I'd recognize anywhere, as well as the barrel of a .38 Special. And holding it was Tommy.

"Shit," I said.

And then he blew my head off.

I was in an elevator, going up. There were no buttons. Halfway through, Khir got on, and stared at me as the doors closed. The elevator continued up, until I heard a ding. Khir stepped out, and held the doors open.

"This is our stop, bro."

"And," I said. "I guess I have to get off, don't I."

"Well," he said. "It's this, or it goes black forever."

And when I stepped out of the elevator, I was greeted by an applause louder than any noise I had ever heard when I was alive, louder than any gun, or any bomb, or any car crash. And the elevator doors closed behind me.

Soundtrack

Sing and Dance - 10 Ft Ganja Plant

HACKER HAPPENINGS

Listed here are some upcoming events of interest to hackers. Hacker conferences generally don't cost a fortune and are open to everyone. If you know of a conference or event that should be known to the hacker community, ***email us*** at **happenings@2600.com** or by snail mail at **Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA.**

Please remember that we need sufficient lead time (a minimum of three months) to list events in the magazine. We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community. All events are subject to change.

January 24-25
Vintage Computer Festival Montreal
Royal Military College of Saint-Jean-sur-Richelieu
Saint-Jean-sur-Richelieu, Quebec, Canada
vcfed.org/vcf-montreal/

February 6-7
CactusCon14
Mesa Convention Center
Mesa, Arizona
www.cactuscon.com

February 11-13
Wild West Hackin' Fest
Hilton Denver City Center
Denver, Colorado
wildwesthackinfest.com

February 14-15
Vintage Computer Festival SoCal
Hotel Fera Anaheim
Orange, California
vcfsocal.com

April 17-19
Vintage Computer Festival East
Infoage Science and History Museums
Wall, New Jersey
vcfed.org

April 24-25
CoCoFEST!
Holiday Inn & Suites Chicago-Carol Stream
Carol Stream, Illinois
www.glensideccc.com/cocofest/

May 15-17
CackalackyCon
DoubleTree at Research Triangle Park
Durham, North Carolina
cackalackycon.org

May 21-22
Ekoparty
Loews Miami Beach Hotel
Miami Beach, Florida
ekoparty.org

May 29-31
Vintage Computer Festival Southwest 2026
Westin Dallas Fort Worth Airport
Dallas, Texas
www.vcfsw.org

June 9-10
RVAsec 15
Richmond Marriott
Richmond, Virginia
rvasec.com

June 24-28
ToorCamp 2026
Doe Bay Resort & Spa
Orcas Island, Washington
toorcamp.org

August 6-9
DEF CON 34
Las Vegas Convention Center West Hall
Las Vegas, Nevada
www.defcon.org

~~August 14-16~~
HOPE 26
~~St. John's University~~
~~Queens, New York~~
hope.net

August 15-16
Maker Faire Hannover
Hannover Congress Centrum
Hannover, Germany
maker-faire.de/hannover

September 24-25
GrrCON
DeVos Place
Grand Rapids, Michigan
grrcon.com

September 25-27
Maker Faire Bay Area
Historic Mare Island Promenade
Mare Island, California
makerfaire.com

Please send us your feedback on any events you attend and let us know if they should/should not be listed here.

Marketplace

For Sale

HACKERBOXES is your monthly subscription box for hardware hacking, DIY electronics, cybersecurity, and hacker culture. Each monthly HackerBox includes a carefully curated collection of projects, components, modules, tools, supplies, and exclusive items. A HackerBox subscription is like having a hacker convention in your mailbox every month. Free online educational material, free domestic shipping, cancel anytime. Visit us at www.➥HackerBoxes.com for workshops, boxes, merch, and more.

BUTTERFLY is an innovative and patented indoor air quality (IAQ) monitoring system including a suite of beautifully designed hardware with glowing wings, integrated software, and a charming narrative that has been developed at Imperial College London over the past 4 years. Our highly qualified UK team has engineered a new standard of accuracy and reliability which meets and exceeds the international WELL standard for buildings. Butterfly IAQ data is consistent and trustworthy, providing for integration with air purification technologies to deliver >40% energy savings in buildings - an industry first. Our products are manufactured in the UK from recycled materials to matchless standards of quality to ensure long term durability and service. 1% of our profits will be donated to the Butterfly Conservation Organization. Until now we have lacked the tools to measure and react to contaminants indoors. Butterfly solves this challenge in a sustainable, trustworthy, and responsible way. We have a carefully considered suite of products which can be flexibly installed in a hub & spoke arrangement to suit a wide variety of buildings: Our secure IOT platform enables clients to monitor and manage the safety, efficiency, and trend of air quality. Check us out at butterfly-air.com

HACKER WAREHOUSE is your one stop shop for hacking equipment. We understand the importance of tools and gear which is why we carry only the highest quality gear from the best brands in the industry. From RF Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers, red teamers, and penetration testers need. Check us out at https://HackerWarehouse.com

***THE RADIO PHONICS LABORATORY:** Telecommunications, Speech Synthesis, and the Birth of Electronic Music* by Justin Patrick Moore, KE8COY. Set your receivers for a mesmerizing story found at the intricate intersection of technology and creativity, spanning a century of discovery from the 1880s to the 1980s. Explore the path of this circuit diagram that connects telegraphy and the invention of the telephone with radio laboratories and the advent of our global communications systems. At the heart of this narrative is the evolution of speech synthesis and the quest to make a machine capable of speech. This groundbreaking innovation not only revolutionized telecommunications but gave birth to a new era of electronic music. Tracing the origins of synthetic speech at places like Bell Laboratories and its applications in various fields, *The Radio Phonics Laboratory* unveils the pivotal role it played in shaping the creative vision of sound pioneers, maverick musicians, and experimental luminaries. This is the story of how electronic music came to be, told through the lens of telecommunications scientists and electrical engineers. This is the story of how electronic music started with the dits and dahs of Morse code and transformed into the blips and bleeps that have captured the imagination of musicians and dedicated listeners around the world. Published by Velocity Press and available in the UK and Europe from velocitypress.uk. In North America find *The Radio Phonics Laboratory* on Bookshop.org, that one big company named after a jungle, and fine bookstores everywhere.

SECPOINT PENETRATOR SOFTWARE: Advanced WiFi Pen Testing (WPA, WPA2, WPS). Comprehensive Vulnerability Scanning & Assessment with 33 profiles. Dark Web Search included. Multi-User Support for MSPs. Fully Customizable Whitelabel Reports, insert your logos, names, and watermarks. Reports delivered in PDF, HTML, & translated into 26 languages. Get 26% OFF - Use Coupon Code 2600 - https://shop.secpoint.com

***HACKS, LEAKS, AND REVELATIONS:** The Art of Analyzing Hacked and Leaked Data,* by Micah Lee: The world is awash with hacked and leaked datasets from governments, corporations, and extremist groups. This data is freely available online and waiting for anyone with an Internet connection, a laptop, and enough curiosity to analyze it. Want to use your hacker skillz to change the world? Check out my new book at hacksandleaks.com. You'll work with real datasets like hacked police docs, chatlogs from a Russian ransomware gang, videos that Jan 6 insurrectionists uploaded with GPS coordinates, and a lot more.

CYBERSECURITY MEETS METAL. Shirts for fictional bands named after malware and threat actors, with all your favorites, including Stuxnet, Conficker, Wannacry, and Socgholish. Literal malwear. https://1336-0ff-by-0ne.myshopify.com/

COOL SOLDERING KITS FOR SALE! TV-B-Gone for turning off TVs in public places. ArduTouch music synthesizer kit for making beautiful music, sound, and noise. And more! Learn and grow and do cool things. Everyone can solder! Step-by-step instructions show you how. All ages, friendly for total beginners. https://CornfieldElectronics.com

CIRCUIT PUNK is a new magazine that embraces the vast world of music technology. It's a home for original schematics and code, DIY guitar pedals/synthesizers, modified and circuit bent instruments, plugins, and much more educational content from readers and industry experts alike. Physical copies (40+ pages, satin paper, full color, gloss cover) are available starting at $6. And the best part? The digital version is completely free. Check it out at circuitpunk.org! 48 East 3rd Street, New York, NY 10003

Announcements

NOPAL MAGAZINE is a literary zine based in central Texas - fiction, news, interviews, cartoons, poems, etc. If you want to be our lone star tech reporter, hit us up. Or just order a copy at nopal.neocities.org. Also in search of print advertisers - our display ads run very cheap.

JOIN THE HACKER WIKI! Share your knowledge and learn from others. Contribute tutorials on computing, Linux, and hacking. Help build the ultimate resource for hackers, by hackers. Collaborate, innovate, and elevate the community. Visit https://➥hack-the-planet.cc to start contributing today!

VAGUEBOOKING is a podcast about life lived online, and our new series "The People's History of the Internet" covers the history of the early Internet and the hackers who shaped it. Tune in for conversations with Phil Lapsley, Lucky225, Rob T Firefly, and many more! Found wherever you get your podcasts and at vaguebooking.net

THE HACKER MINDSET offers a fresh perspective on using your hacking skills beyond the digital world. Garrett Gee reveals how to apply these talents to life's broader challenges. Discover how to hack your way to success in every aspect of your life. Now in print and available at your local book store and major book retailers. Read more at https://hackermindsetbook.com/2600

STRAY POINTERS is an interview and discussion podcast focusing on people who are doing or experiencing amazing things in a variety of subject areas in tech and the arts. Please look for it on your favorite podcast site or stop by straypointers.com for a complete list of episodes.

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.

➥com/offthehook. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Your feedback on the program is always welcome at oth@2600.com. New for the pandemic: *Off The Hook Overtime,* Wednesdays at 8:00 pm ET on youtube.com/channel2600. Call in at +1 802 321 HACK!

Services

KOLLER SECRET: The first truly hidden app for Android. No launcher. No icon. Nothing to click on. The only way to open it is by entering a custom Android secret code on your dial pad. It's completely hidden, perfect for keeping private photos, videos, and sensitive files secure. Built for activists, journalists, hackers, and anyone working in sensitive environments, such as government officers, Secret Service agents, etc. We strictly adhere to a privacy-first, anti-surveillance policy. No ads. No tracking. No logging. No data collection. Not even Internet required. Koller Secret Pro offers the same ultimate privacy with advanced security features, including AES-256 encryption, Kill Switch to automatically wipe out your data in an emergency, and Backup & Restore to recover it later when it's safe. Find us on Google Play and try it out! BONUS for *2600* readers: Leave us a review on Google Play for either version of the app, then DM us at 2600@iotrusted.com. We will immediately send you a promo code to purchase Koller Secret Pro for free (or gift it to a friend if you already paid for one). Found a critical bug? Report it to us and receive another free promo code as thanks. More info: https://koller.iotrusted.com/?download

HAM RADIO IS THE PERFECT HOBBY FOR HACKERS, and KB6NU's "No Nonsense" amateur radio license study guides make it easy to get your Technician Class license or upgrade to General Class or Extra Class. They clearly and succinctly explain the concepts, while at the same time, give you the answers to all of the questions you need to pass the test. The PDF version of the Technician Class study guide is FREE, but there is a small charge for other versions. All of the e-book versions are available from kb6nu.com/study-guides. Print versions are available from Amazon. Email cwgeek@kb6nu.com for more info.

LOCKPICKING101.COM is open to hackers wanting to learn physical security and the insides and out of locks and lock picking. Register to join one of the oldest Locksport communities online.

AFFORDABLE WEB HOSTING & SERVERS: Tired of faceless mega-hosts that don't seem to care if your site is down? NodeSpace Hosting is a small, independent provider offering shared & reseller hosting, email, domains, SSL, VPS, and bare metal servers at sane prices. Real humans. No nonsense. See why others love our hosting. Use promo code 2600424 for 10% off recurring discount any shared or reseller plan, VPS, or in stock bare metal server. We also provide free migrations from other service providers! https://www.nodespace.com

ICONOCLASTIC RESEARCH LIBRARY - Visit us in San Francisco to read *2600* in hard copy going back many years! Take a bite out of *Byte,* or study radio science. Stacks at the Prelinger Library offer hundreds of feet of books about the history of computing and related technologies, wired in with dozens of other subjects. Browse vintage *Science and Mechanics* and *Computers and People,* or get lost in the zine archives. You may discover a topic you didn't know existed. We offer tea to visitors and collect no information that visitors do not volunteer in our guestbook. Location and hours as well as remote browsing environment can be found at www.prelingerlibrary.org. Half the hosting consortium are amateur radio operators. Not a lending library, though we welcome photography and scanning on site, and all items digitized and hosted by our allies at Internet Archive (www.archive.org) are freely downloadable.

ANTIQUE COMPUTERS. From Altos to Zorba and everything in between - Apple, Commodore, DEC, IBM, MITS, Xerox... vintagecomputer.net is full of classic computer hardware restoration information, links, tons of photos, video, document scans, and how-to articles. A place for preserving historical computers, maintaining working machines, running a library of hard-to-find documentation, magazines, SIG materials, BBS disks, manuals, and brochures from the 1950s through the early WWW era. http://www.vintagecomputer.net

BUSINESS AND TECHNICAL ADVICE AND SOLUTIONS. Got a tough business problem? Need a creative, impactful solution from somebody who understands the tech? I offer strategies and solutions for everything from business growth to data visualization, with a hacker mindset for tackling challenges. Business, startup, or just looking to make some money with your skills, I can help you out. Let's chat. Visit avc.consulting or email hello@avc.consulting and mention *2600.*

DO YOU HAVE A LEAK OR A TIP that you want to share with *2600* securely? Now you can! *2600* is using SecureDrop for the submission of sensitive material - while preserving your anonymity. Anonymous tips and documentation are where many important news stories begin. With the SecureDrop system, your identity is kept secret from us, but we are able to communicate with you if you choose. It's simple to use: connect to our special .onion address using the Tor browser (2600.securedrop.tor.onion), attach any documents you want us to see, and hit "Submit Documents"! You can either walk away at that point or check back for a response using a special identification string that only you will see. For all the specifics, visit https://www.2600.com/securedrop (you can see this page from any browser). For more details on SecureDrop itself, visit https://securedrop.org. (SecureDrop was developed by Aaron Swartz, Kevin Poulsen, and James Dolan and is a part of the Freedom of the Press Foundation, used by journalists and sources worldwide.)

TOP TIER FULL STACK IT CONSULTING for all your needs - competitive pricing! We specialize in providing over 27 years of experience in delivering top tier IT consulting services. Our full stack runs the gamut all the way from software, hardware, network and security engineering, and in a wide range of fields such as marketing, art & design, and research. Services include: IT Infrastructure and Network Design (full system and network architecture design using open-source technologies, white-glove support for implemented solutions), Security Services (comprehensive incident response services, security architecture and consultancy, custom tool development for security operations), Legacy System Support (maintenance and support for legacy systems, including those crucial for business continuity), Software Development (custom software development for specific needs, including physical access control and blockchain), Consulting and Advisory (IT and security consulting with a focus on strategic advice and incident response; business development consulting, particularly in the tech and e-commerce sectors), Specialized Projects (development and support for unique and challenging tech projects, such as those beyond what mainstream solutions like Zillow can offer. 31337 IT Solutions http://31337itsolutions.com/

CALL INTO THE PHONE LOSERS OF AMERICA'S telephone network interface and hack into our collection of answering machines from the 80s, 90s, and 2000s. Listen to episodes of Joybubble's "Stories and Stuff," old telephone recordings, adventure choosing games, and more! Dial 505-608-6123 or 845-470-0336.

HAVE YOU SEEN THE *2600* STORE? All kinds of hacker clothing, back issues, and HOPE stuff! We accept Bitcoin and Google Wallet, along with the usual credit cards and PayPal. It's great for giving out presents with a hacker theme - or gift cards are available for those who'd rather make their own choices. The store is constantly getting bigger and more interesting. Please come pay us a visit! store.2600.com or 2600.store

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. **We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril.** All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include a copy of your address label/envelope or a receipt/customer number so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to marketplace@2600.com.

Deadline for Spring issue: 2/27/26.

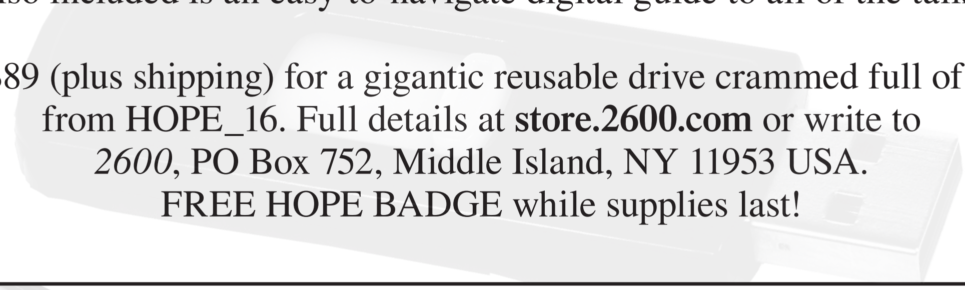
THE HOPE_16 FLASH DRIVE

If you missed this year's historic conference, we've got you covered!
All of the talks are available on this single drive.

Each talk is available as a video or audio file and can be copied to any device of your choosing or shared with as many people as you wish.

HOPE_16 was our latest conference at St. John's University in Queens, New York City. It was the first conference to take place in our new annual format. You can experience or recapture the excitement that was in the air for all three days. A full lineup of talks can be found at xvi.hope.net.

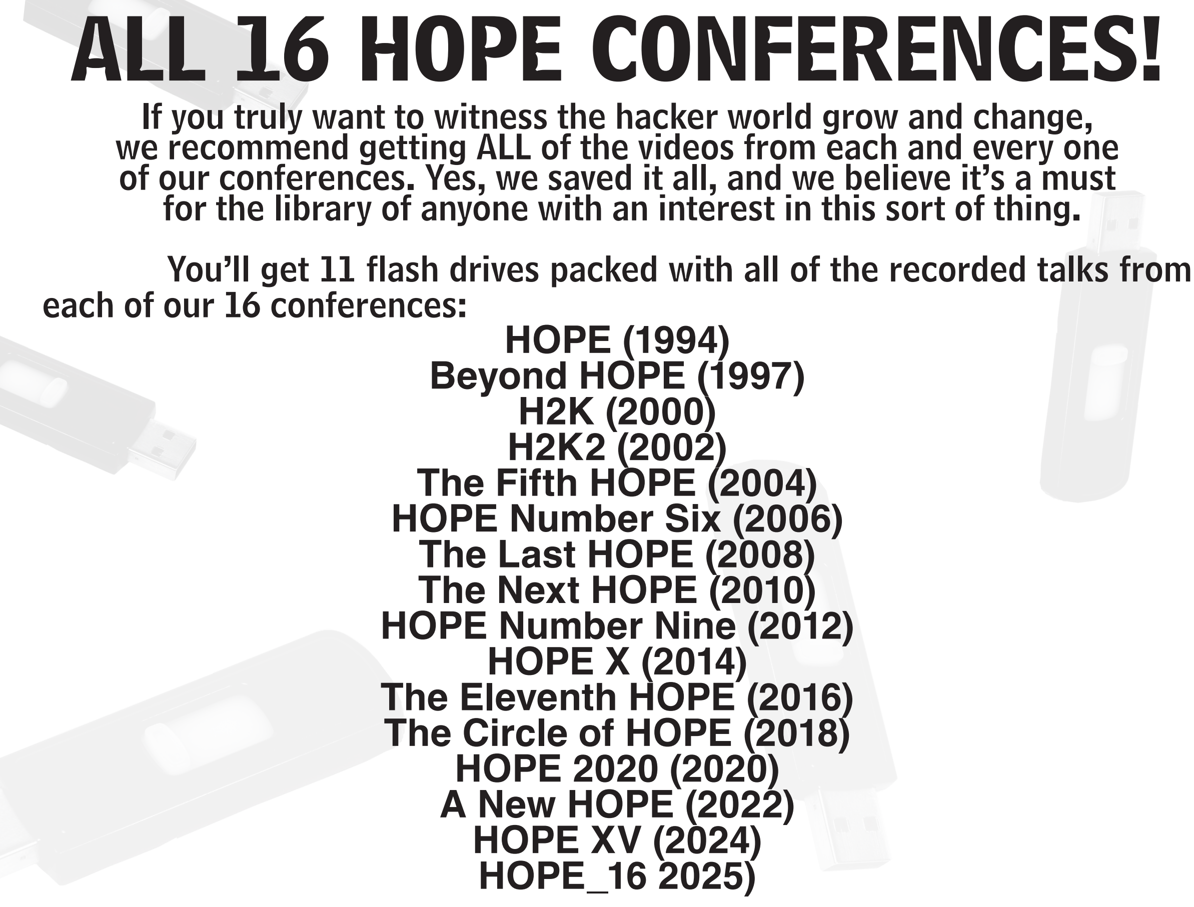
Also included is an easy-to-navigate digital guide to all of the talks.



Just $89 (plus shipping) for a gigantic reusable drive crammed full of talks from HOPE_16. Full details at **store.2600.com** or write to
2600, PO Box 752, Middle Island, NY 11953 USA.
FREE HOPE BADGE while supplies last!

ALL 16 HOPE CONFERENCES!

If you truly want to witness the hacker world grow and change, we recommend getting ALL of the videos from each and every one of our conferences. Yes, we saved it all, and we believe it's a must for the library of anyone with an interest in this sort of thing.



You'll get 11 flash drives packed with all of the recorded talks from each of our 16 conferences:

HOPE (1994)
Beyond HOPE (1997)
H2K (2000)
H2K2 (2002)
The Fifth HOPE (2004)
HOPE Number Six (2006)
The Last HOPE (2008)
The Next HOPE (2010)
HOPE Number Nine (2012)
HOPE X (2014)
The Eleventh HOPE (2016)
The Circle of HOPE (2018)
HOPE 2020 (2020)
A New HOPE (2022)
HOPE XV (2024)
HOPE_16 2025)

Each conference comes with an easy-to-navigate digital guide and all talks are DRM-free, meaning you can copy them and view them anywhere (and reuse all of these drives for other things!).

You can get it all for $489 plus shipping. Full details at store.2600.com or write to *2600*, PO Box 752, Middle Island, NY 11953 USA.

"I build things, in order to enhance our information commons. I then seek to give those things away. What shall we build next, together?" - Greg Newby

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
typ0

Cover
Dabu Ch'wald

Office Manager
Tampruf

Infrastructure
flyko

Network Operations
phiber, olssy

Broadcast Coordinator
Juintz

IRC Admins
honeyp0t, r0d3nt, dclaw

Facebook Team
astrutt, Cryovato, TechnoMage, danixdefcon5, ItsTehPope, JWiley

Inspirational Music: Jesse Welles, The Who, Sunidhi Chauhan, Alicia Bridges, Jimmy Cliff
Shout Outs: Ilana, Trey & Matt, Cody Kociemba
Welcome: Zine
RIP: Estragon, Karamoon, Delchi, NotLarry

***2600* is written by members of the global hacker community. You can be a part of this by sending your submissions to articles@2600.com or the postal address below.**

***2600** (ISSN 0749-3851, USPS # 003-176) is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.*

POSTMASTER:
Send address changes to: *2600,*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. & Canada - $31 individual,
$60 corporate (U.S. Funds)
Overseas - $44 individual, $75 corporate
Digital (PDF and EPUB) - $19.99 at
store.2600.com

BACK ISSUES:
Individual issues for 1988-2024 are $7.25 each when available. Shipping added to overseas orders. All back issues (1984-2024) available digitally as annual digests and individually in PDF format from 2018 on at store.2600.com

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

Mastodon: @2600@mastodon.online Bluesky: @2600.com Remains of Twitter: @2600

***2600* Office/Fax Line: +1 631 751 2600**

MEETINGS

**_2600_ MEETINGS ARE THE BEST WAY TO MEET FELLOW HACKERS!
KEEP CHECKING THE WEBSITE BELOW FOR MORE UPDATED LISTINGS
AS WELL AS INFO ON HOW TO START YOUR OWN MEETING!**

ARGENTINA

Buenos Aires: Bodegón Bellagamba, Armenia 1242. 1st table to the left of the front door.

Parana: El Estribo Choperia, Italia 255 (Club Recreativo)

Saavedra: Pizzeria La Farola de Saavedra, Av. Cabildo 4499. 7 pm

AUSTRALIA

Adelaide (2600adelaide.bsky.social): By the payphone outside State Library. Corner N Terrace and Kintore Ave. 6 pm

Melbourne: Oxford Scholar RMIT, 427 Swanston St. 6 pm

Sydney (`www.meetup.com/sydney-2600/`**):** Club York Sydney, 99 York St. 6:30 pm

CANADA

Ontario

%Toronto: Victory Cafe, 440 Bloor St W. 6 pm

Waterloo: Conestoga Mall Food Court, 550 King St N.

Quebec

Montreal (Westmount): Food court, Westmount Square.

COLOMBIA

Medellin: El Primer Parque de Laureles. 6 pm

CZECHIA

Prague: Legenda Pub. 6 pm

FINLAND

Helsinki: Mall of Tripla food court (2nd floor).

FRANCE

Paris: Place de la République, 1st floor of the Burger King, 10th arrondissement.

IRELAND

Dublin: The Molly Malone Statue on Suffolk St. 7 pm

JAPAN

Tokyo: Beemars, Kabukicho, 2 Chome-27-12 Shinjuku Lee Building #2 3rd floor. 7 pm

KAZAKHSTAN

Almaty: Hoper's Bar, 93a Prospekt Gagarina.

PORTUGAL

Lisbon: Julio's Eat Drink Enjoy, Av Elias Garcia 19B. 7 pm

RUSSIA

Petrozavodsk: Good Place, pr. Pervomayskiy, 2. 7 pm

SPAIN

Madrid (`2600.madrid`**):** Fotos y Tapas, Calle del Dr. Piga, 7, Centro, Lavapies. 9 pm

SWEDEN

Malmo (`malmo.2600.se`**) (_@2600Malmo@mastodon.online_)** (@2600Malmo)**:** FooCafé, Carlsgatan 12A.

Stockholm (`stockholm.2600.se`**) (_@2600stockholm@mastodon.social_)** (@2600Stockholm)**:** Urban Deli, Sveavägen 44.

U.K.

England

Birmingham (2600brumbtek.bsky.social): The Wellington in City Centre.

Bournemouth (`www.bournemouth2600.org/`**)** (@bournemouth2600)**:** The Goat & Tricycle, 27-29 W Hill Rd. 6:30 pm

Cheltenham (`2600cheltenham.uk/`**)** (@2600Cheltenham)**:** Bottle of Sauce, Ambrose St. 6:30 pm

London (`2600.london`**)** (@London_2600)**:** Angel Pub, 61 St Giles High St, outdoors at the red telephone box. 6:30 pm

Manchester (@2600Manchester)**:** Piccadilly Taps, upstairs room. 6 pm

Scotland

Glasgow (`www.2600glasgow.com`**) (_@2600@glasgow.social_):** The Geek Rooms, 151 Bath Ln. 6 pm

URUGUAY

Montevideo: MAM Mercado Agricola de Montevideo, José L Terra 2220, Choperia Mastra. 7 pm

U.S.A.

Alabama

Huntsville: Parkway Place Mall food court near the Bitcoin ATM.

Arizona

Phoenix (Tempe) (`www.phx2600.org/`**)** (@PHX2600)**:** Escalante Community Center, 2150 E Orange St. 6 pm

Prescott: Merchant Coffee, 218 N Granite St.

Arkansas

Fort Smith (`www.fs2600.net`**):** Fort Smith Coffee Company, 70 S 7th St. 7 pm

California

Fullerton: (`www.meetup.com/OC2600/`) 23b Shop, 418 E Commonwealth Ave, Unit 1. 7 pm

Los Angeles (`2600.la`**) (@LA2600):** Union Station inside the main entrance by Alameda St near Traxx Bar. 6 pm

Sacramento: La Venadita, 3501 3rd Av. 6 pm

San Francisco: 4 Embarcadero Center, ground level by info kiosk. 6 pm

San Jose: Outside the MLK Library, 6 pm

Colorado

Denver (`denver.2600.horse`**)** (@denver2600)**:** Denver Pavilions. 6 pm

Fort Collins: Starbucks, 4218 College Ave. 7 pm

Connecticut

Watertown: (`2600meetingct.wordpress.com/`) CT Hackerspace, 30 Echo Lake Road. 6 pm

District of Columbia

(see **Arlington, Virginia**)

Florida

Boca Raton: Living Green Cafe on Federal Hwy.

Jacksonville: The Silver Cow, 929 Edgewood Ave S.

Orlando: Miller's Ale House, 2600 E Colonial Dr.

Georgia

Atlanta (`atl2600.org`**) (@Atl2600):** Lenox Square Mall, 3393 Peachtree Rd NE. 6 pm

Illinois

Oak Lawn (`oaklawn2600.com`**)** (@OakLawn2600)**:** The Meta-Center, 4606 W 103rd St, Ste B.

Urbana-Champaign: Harvest Market mezzanine. 6 pm

Indiana

South Bend (`sb2600.com`**):** Cloud Walking Cafe.

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall. 6 pm

Louisiana

New Orleans: Z'otz Cafe, 8210 Oak St #2042.

Maine

Bangor (Hermon) (maine2600.bsky.social) (@2600Bangor)**:** Bangor Makerspace, 34 Freedom Pkwy

Massachusetts

Boston (Cambridge) (@2600boston)**:** The Garage, Harvard Square, food court area. 7 pm

Hyannis: Nifty Nate's, 246 North St.

Michigan

Lansing (lansing2600.bsky.social): The Fledge, 1300 Eureka St. 6 pm

Minnesota

Bloomington: (`mn2600.org`) Mall of America, north food court by Burger King. 6 pm

Missouri

St. Louis: Arch Reactor Hackerspace, 2215 Scott Ave.

New Hampshire

Peterborough (`nh2600.neocities.org/`**) (_@nh2600@defcon.social_):** Mi Jalisco, 19 Wilton Rd. 7 pm

New Jersey

Bridgewater (`2600nj.org/`**) (@2600NJ):** Bridgewater Commons Mall, food court near drinking fountains.

New York

Albany: UAlbany ETEC Bldg, 1220 Washington Ave. 6 pm

New York (`nyc2600.net`**) (_@NYC2600@mastodon.social_):** Citigroup Center, 53rd St & Lexington Ave, food court.

Rochester (`rochester2600.com`**)** (@roc2600)**:** Global Cybersecurity Institute, 78 Rochester Institute of Technology. 7 pm

North Carolina

Raleigh (rtp2600.bsky.social) (_kolektiva.social/@RTP2600_) (@rtp2600)**:** Transfer Co Food Hall, 500 E Davie St. 7 pm

Ohio

Columbiana: Brew Lounge Beer Company.

Youngstown: Denny's Restaurant, 4020 Belmont Ave. 6 pm

Oklahoma

Oklahoma City: Big Truck Tacos, 530 NW 23rd St. 6 pm

Oregon

Portland: Sizzle Pie Central Eastside, 624 E Burnside St. 7 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St.

Lancaster (Columbia) (`pa2600.wixsite.➥com/pa2600`)**:** Trio Bar & Grill. 3 pm

Philadelphia (`philly2600.net/`) **(_jawns.club/@philly2600_):** Iffy Books, 404 S 20th St. 6 pm

Tennessee

Memphis (`memsec.info`**):** FIT Building at the University of Memphis, Room 225

Texas

Austin (`atx2600.org`**) (@atx2600):** Central Market upstairs mezzanine, 4001 N Lamar Blvd. 7 pm

Dallas: The Wild Turkey, 2470 Walnut Hill Ln #5627.

Houston: (`www.hou2600.org/`**):** Taco Cabana, 3905 Kirby. 7 pm

Lubbock: (`2600Lbk.com`) **(@2600lbk.com)** (@2600Lbk)**:** Mad Hatter's House of Games, 1507 Texas Ave.

San Antonio: PH3AR/Geekdom, 110 E Houston St. 6 pm

Utah

Salt Lake City: 801labs Hackerspace 353 E 200 S, Ste B. 6 pm

Virginia

Arlington: First floor food court by Sakina's at Fashion Centre at Pentagon City, 1100 S Hayes St.

Hampton: Barnes & Noble cafe, Peninsula Town Center.

Washington

Seattle: Seattle Interactive Media-Lab, 3131 Western Ave #421. 6 pm

Spokane: Starbucks near Wellesley & Division (across from North Town Mall).

West Virginia

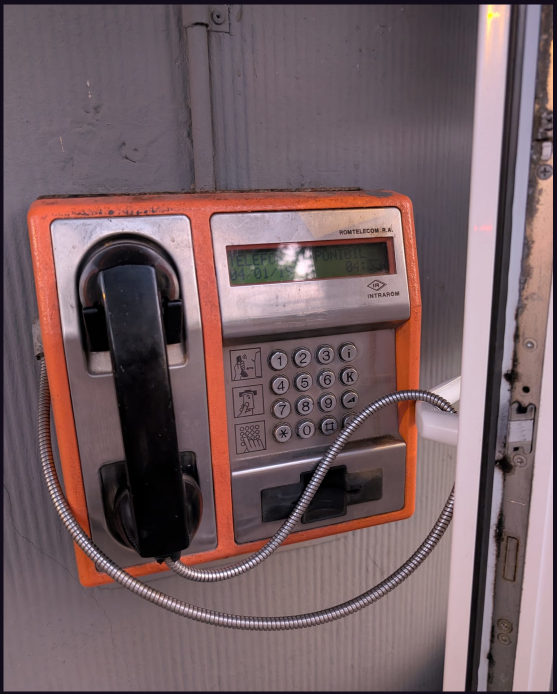
Charleston: KDE Technology, 111 Hale St.

All meetings take place on the first Friday of the month. Unless otherwise noted, _2600_ meetings begin at 5 pm local time. Follow @2600meetings.bsky.social on Bluesky and let us know your meeting's `website` **and/or Bluesky, _Mastodon_, or** Twitter **handle so we can stay in touch and share them here! To start a meeting in your city, DM us or send email to meetings@2600.com.**

% 2nd Monday

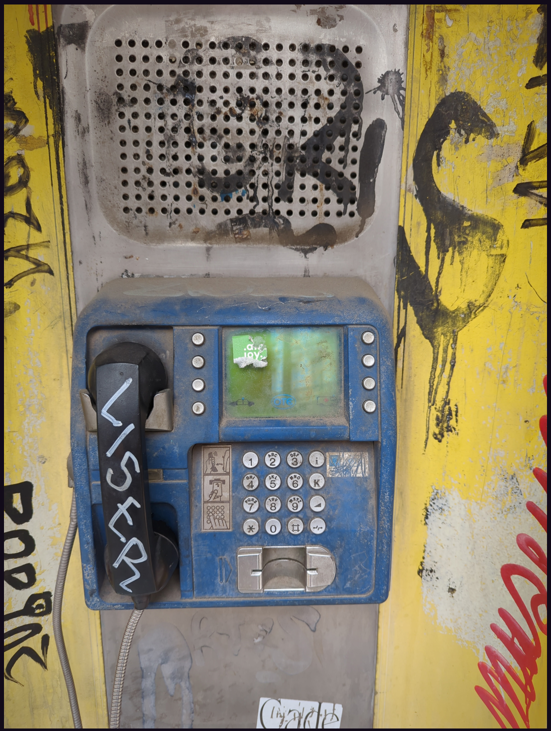
www.2600.com/meetings

Payphones of Eurasia



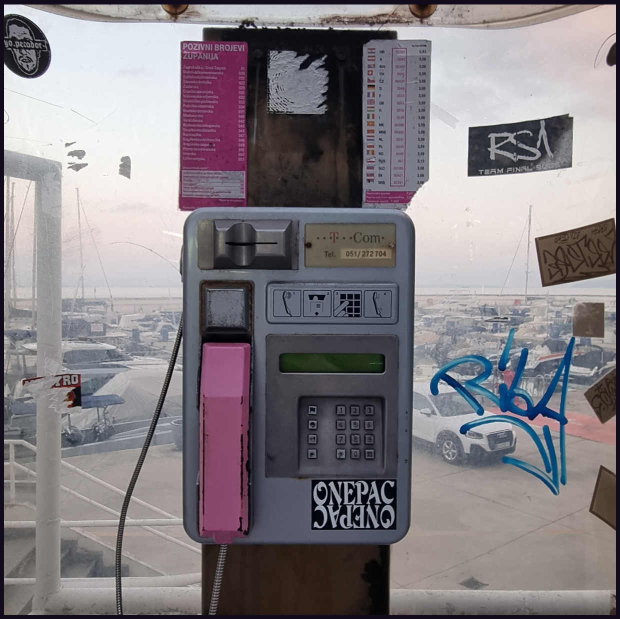
Romania. If you look carefully, you can see this Brasov phone is actually being used to hold a door open. Despite that, it still works, although the date on the display is way off and phone cards for this model haven't been on sale for over a decade.

Photo by Radu Paraschivescu



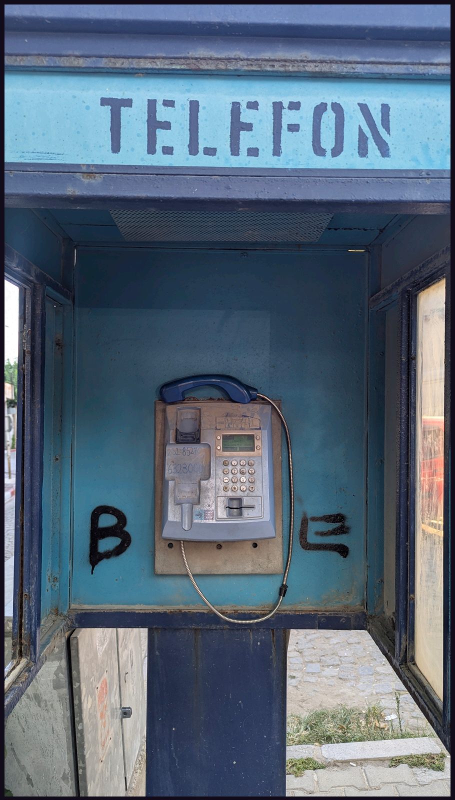
Greece. This rugged phone with accompanying free expression was found in the anarcho-revolutionary neighborhood of Exarcheia in Athens.

Photo by TL Popejoy



Croatia. Operated by Hrvatski Telekom, which is majority-owned by Deutsche Telekom, hence the familiar T-Mobile logo. Seen in Primorje-Gorski Kotar County by the water.

Photo by Indro Neri

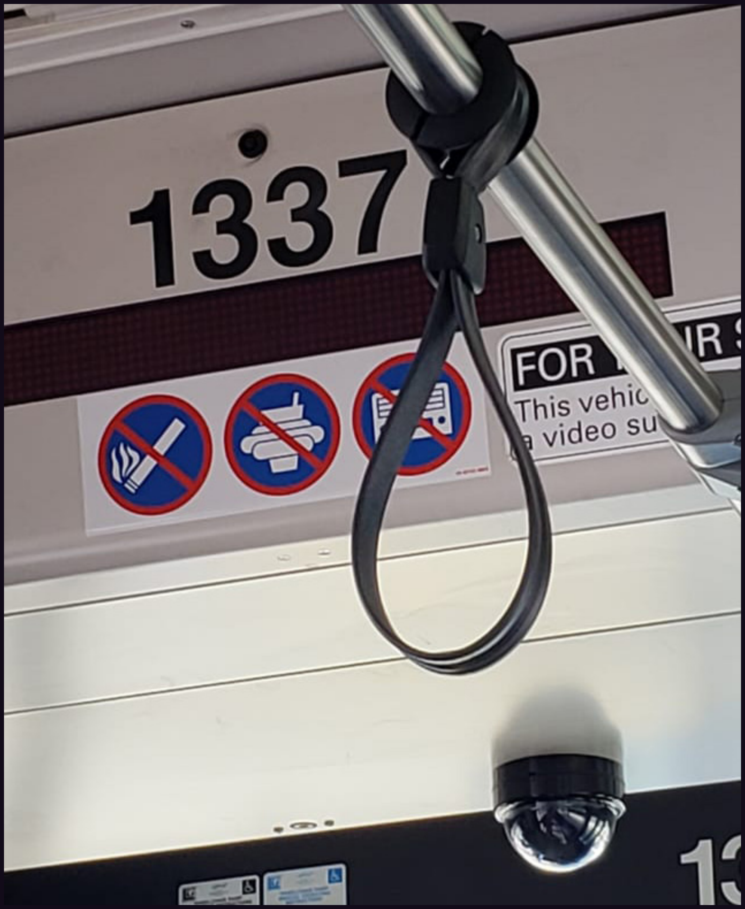


Türkiye. While a small part of the country (formerly known as Turkey) is in Europe, this phone is located in Bergama, which is in Asia and hence resulted in the title of this page. It actually works, but it's really filthy.

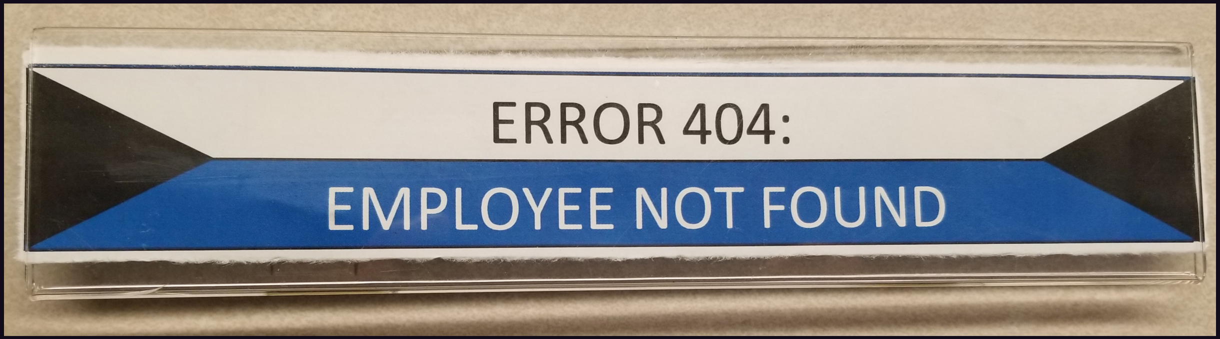
Photo by L&L

Visit **www.2600.com/payphones** to see our foreign payphone photos!
(or turn to the inside front cover to see more right now)

The Back Cover Photos



Every now and then you find the coolest bus in the entire city. This one was found by **sigflup synasloble** in Minneapolis. We wonder if the driver knew what they had.



A while back, **Matthew Jennings** quit his job and decided to replace the name tag on his cube. A former coworker snapped this picture after it had hung there without notice (other than by the cool kids) for weeks.

If you've spotted something that has "2600" in it or anything else of interest to the hacker world (such as funny uses of "hacker," "unix," "404," you get the idea...), take a picture and send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed. Make sure and tell us where you spotted your subject along with any other info that makes it interesting - many photos are eliminated due to lack of detail.

Email your submissions to articles@2600.com or use snail mail to
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) and a *2600* t-shirt of your choice.