Security Now! #1032 - 07-01-25

Pervasive Web Fingerprinting

This week on Security Now!

• Let's Encrypt drops its long-running email notifications. • Microsoft's new "Unexpected Restart Experience". • Microsoft's response to last year's massive CrowdStrike outage. • Windows 10's extended service updates will sort of be free. • Russia-sold iPhones MUST include the RuStore app. • Lyon, in France, says bye-bye to Windows. Hello to Linux. • The US Gov gets more serious about memory-safe languages. • A new unbelievable AI malware scanner evaSion technique. • A new pair of Cisco 9.8 and 10.0 vulnerabilities. • The current state of post-Elon government cybersecurity. • PNGv3, Swift on Android, and the Samsung email purge. • Andy Weir's "Hail Mary" movie trailer. • And a close look at the pervasiveness of web browser tracking fingerprinting.

We're left with the impression that
"Fire Exit Only" is not taken very seriously.

Security News

Let's Encrypt terminated its certificate expiration email service

This notice from Let's Encrypt made a lot of sense to me. Their announcement last Thursday (https://letsencrypt.org/2025/06/26/expiration-notification-service-has-ended/) said:

> Since its inception, Let's Encrypt has been sending expiration notification emails to subscribers that have provided an email address to us via the ACME API. This service ended on June 4, 2025. The decision to end the service is the result of the following factors:
>
> - Over the past 10 years more and more of our subscribers have been able to put reliable automation into place for certificate renewal.
> - Providing expiration notification emails means that we have to retain millions of email addresses connected to issuance records. As an organization that values privacy, removing this requirement is important to us.
> - Providing expiration notifications costs Let's Encrypt tens of thousands of dollars per year, money that we believe can be better spent on other aspects of our infrastructure.
> - Providing expiration notifications adds complexity to our infrastructure, which takes time and attention to manage and increases the likelihood of mistakes being made. Over the long term, particularly as we add support for new service components, we need to manage overall complexity by phasing out system components that can no longer be justified.
>
> For those who would like to continue receiving expiration notifications, we recommend using a third party service such as Red Sift Certificates Lite (formerly Hardenize). Red Sift's monitoring service providing expiration emails is free of charge for up to 250 certificates. More monitoring options can be found at: https://letsencrypt.org/docs/monitoring-options/
>
> We have deleted the email addresses provided to Let's Encrypt via the ACME API that were stored in our CA database in association with issuance data. This doesn't affect addresses signed up to mailing lists and other systems. They are managed in a separate ISRG system unassociated with issuance data.
>
> Going forward, if an email address is provided to Let's Encrypt via the ACME API, Let's Encrypt will not store the address but will instead forward it to the general ISRG mailing list system unassociated with any account data. If the email address has not been seen before, that system may send an onboarding email with information about how to subscribe to various sources of updates.
>
> If you'd like to stay informed about technical updates and other news about Let's Encrypt and our parent nonprofit, ISRG, based on the preferences you choose, you can sign up for our email lists below:
>
> - Brighter Bytes: the ISRG Newsletter
> - Let's Encrypt Technical Updates
> - Let's Encrypt Service Statistics
> - Prossimo: Updates about our memory safety project
> - Divvi Up: Updates about our privacy-respecting metrics project

The link at the top of page 2 of the show notes to this announcement page has a form into which anyone can supply an email address and subscribe to any of those newsletters and updates.

As I noted, this makes a lot of sense to me. 90-day certificates would only require four or five

pieces of email per year. That's not insane for a single Let's Encrypt user. But from Let's Encrypt's standpoint, as their service has grown until they are now providing certificates for nearly two out of every three websites, that becomes a great deal of email. And as certificate life continues down its current trajectory, anyone who doesn't have certificate re-issuance automation working correctly is not going to be saved by email reminders.

Microsoft's "Unexpected Restart Experience"

We're not calling it a Windows "crash" anymore. No. To everyone's great relief, Windows will no longer crash. However, Windows users may experience what Microsoft is now officially calling an "unexpected restart experience." This puts me in mind of Space-X's term for one of their rockets exploding on the launchpad. You may have heard this referred to as "an Unplanned Rapid Disassembly" with the abbreviation URD, or sometimes as an RUD, which stands for Rapid Unplanned Disassembly. Also, Microsoft's famous BSOD – Blue Screen Of Death – is changing its appearance but, blessedly, not its abbreviation. They've changed the screen background color to Black. So now the official "Unexpected Restart Experience" will be unofficially the Black Screen Of Death. Here's what Microsoft explained under the heading *"Now it's easier than ever to navigate unexpected restarts and recover faster"* in their *"Windows Experience Blog"* last Thursday, they wrote:

> *A key trait of a resilient organization is the ability to maintain productivity and minimize disruptions. But when unexpected restarts occur, they can cause delays and impact business continuity. This is why we are streamlining the* ***unexpected restart experience.*** *We are also adding quick machine recovery, a recovery mechanism for PCs that cannot restart successfully. This change is part of a larger continued effort to reduce disruption in the event of an unexpected restart.*

This sure sounds suspiciously like a response to the massive CrowdStrike outage that occurred nearly a year ago last July 19th of 2024: "*a recovery mechanism for PCs that cannot restart successfully"*. Hmmmmm. Anyway, Microsoft continues:

> *The Windows 11 24H2 release included improvements to crash dump collection which reduced downtime during an unexpected restart to about two seconds for most users. We're introducing a simplified user interface (UI) that pairs with the shortened experience. The updated UI improves readability and aligns better with Windows 11 design principles, while preserving the technical information on the screen for when it is needed.*
>
> *The simplified UI for unexpected restarts will be available starting later this summer on all Windows 11, version 24H2 devices.*
>
> *In the case of consecutive unexpected restarts, devices can get stuck in the Windows Recovery Environment (Windows RE), impacting productivity and often requiring IT teams to spend significant time troubleshooting and restoring affected devices. This is where quick machine recovery* ***(QMR)*** *can help. When a widespread outage affects devices from starting properly, Microsoft can broadly deploy targeted remediations to affected devices via Windows RE—automating fixes with QMR and quickly getting users back to a productive state without requiring complex manual intervention from IT.*

Yeah… that's definitely Microsoft's response to and solution for last year's massively widespread CrowdStrike event. That is certainly good news. They conclude:

*We are excited to announce **QMR** will be generally available later this summer together with the renewed **unexpected restart functionality.** QMR supports all editions of Windows 11, version 24H2 devices. It is enabled by default for Windows 11 Home devices; IT admins will be in full control and can enable it on devices running Windows 11 Pro and Enterprise. Later this year, Microsoft will release additional capabilities for IT teams to customize QMR.*

So we have quicker recovery from "unexpected restarts", the tired old blue screen turning black, and the response to preventing another widespread CrowdStrike-like event. That's all great.

As I'm sure every one of our listeners knows, a very important and interesting date is creeping toward us. Microsoft has previously announced that they will stop providing free access to many more years of Windows 10 security updates – meaning fixes for their own software mistakes – but that up to three years of updates can be purchased from them. So now we'll be paying Microsoft to cure the vulnerabilities that they have left behind in Windows 10.

Of course, normally we could just upgrade to Windows 11. The only problem with that, is that despite the fact that any machine that's able to run Windows 10 can run Windows 11 – after all, Microsoft tells us that Windows 11 is faster than Windows 10, so it would run better on the same hardware – but Microsoft long ago arbitrarily decided to attempt to force their Windows 10 users to abandon their existing perfectly working hardware by setting higher machine requirements for Windows 11 than for Windows 10. Anyway, I know I'm a broken record about this, but it feels SO WRONG to me.

But here we are today with the end of service life of Windows 10 approaching while more than half of all Windows systems are still running Windows 10. How can that be? Well, it must either be that Windows 10 users do not want to upgrade, or they cannot. But this leaves Microsoft with a practical problem. As it is, it appears that somewhere around half a billion PCs are just going to keep right on running Windows 10, even after Microsoft deliberately terminates support.

And that's not a good look for Microsoft because it's their own software security bugs that they are saying they refuse to patch for somewhere around half a billion PCs. They have those patches ready to go since they will be selling them to those who are willing to pay. But just not to everyone else who is equally deserving and will become increasingly vulnerable over time as new Windows 0-days are discovered in the unmaintained Windows 10 code base.

So it wasn't too surprising when we received the news last Tuesday the 24th that Microsoft had blinked and figured out a face-saving way of punting on the termination of patches, at least for the first year of patch outage. Here's what Microsoft wrote last Tuesday:

Extended Security Updates for Windows 10:

For individuals: An enrollment wizard will be available through notifications and in Settings, making it easy to enroll in ESU directly from your personal Windows 10 PC. Through the enrollment wizard, you'll be able to choose from three options:

- *Use Windows Backup to sync your settings to the cloud—at no additional cost..*
- *Redeem 1,000 Microsoft Rewards points—at no additional cost..*
- *Pay $30 USD (local pricing may vary).*

Once you select an option and follow the on-screen steps, your PC will automatically be enrolled. ESU coverage for personal devices runs from Oct. 15, 2025, through Oct. 13, 2026.

Starting today, the enrollment wizard is available in the Windows Insider Program and will begin rolling out as an option to Windows 10 customers in July, with broad availability expected by mid-August.

So, in other words, if you agree to use Windows Backup to sync your settings to Microsoft's cloud, you will be entitled to the first year of ESU – Extended Security Updates – at no charge. Or, if you somehow have 1,000 Microsoft Reward points accumulated you can, instead, cash them in for that first free year. Otherwise, it'll be $30 USD. I just checked and I somehow have earned 1,944 points despite using Edge and Bing as little as humanly possible. I do recall that I gave Edge a try for awhile, seduced by its support for vertical tabs. But it did something to move me back to Firefox. Perhaps while I was there I racked up some Microsoft Brownie points. But, hey, I'll be glad to use them to keep updates flowing because I'm sure as heck not paying Microsoft for updates as a matter of principle.

So this new policy is sort of tricky. No one can claim that they're being left high and dry without ongoing security patches and being extorted for them, since allowing Microsoft to backup one's computer seems like a pretty good deal for free and then the patches will keep right on rolling in.

And, lord knows, they are really pushing this cloud backup solution of theirs. Every time one of my Windows 10 machines gets a big update it resets the Win10 setup and I again need to tell Microsoft that, no, I don't want to synchronize Windows with my Android phone (which I don't own), I'm forced to decline XBOX nonsense and then fight with them to not have them backup my machine to the cloud, thank you very much.

So, in any event, Windows users who have a Microsoft account can open Edge, as I just did, and click their icon or picture in the upper right... and you'll see your current Microsoft Rewards points total on the panel that drops down. If you have more than 1,000 points you should be able to keep updates flowing in. And if you're an Edge and Bing user you may find that yourself with a wealth of points that you'll be able to use to keep many Win10 machines happily humming along and fully patched, at least for this first year until mid October 2026, at no cost.

Pretty tricky, Microsoft. 🙂

Russian-sold iPhones to get the RuStore app

An article on the Russian "Izvestia" site published last Wednesday has the headline "Apple of contention: The State Duma ordered Apple to install RuStore on devices." For those not well versed in Russian government structure (as I was not), the State Duma is the lower house of the Federal Assembly of Russia, which is the national legislature of the Russian Federation. It's similar in function to other lower houses of parliament in bicameral systems. The article said:

State Duma deputies have ordered the American corporation Apple to install the unified Russian RuStore app store on their devices when selling in Russia.

Deputies of the State Duma in the second and third readings adopted a law that, from September 1, 2025, will prohibit Apple and other manufacturers of technically complex products from restricting the installation and use of the Russian RuStore app store on smartphones and tablets sold in Russia.

The law obliges devices to provide the ability to install, update, and pay for applications through RuStore, and also prohibits blocking programs from third-party sources and imposing restrictions on payment methods and pricing policies. These measures are aimed at combating the anti-competitive practices of foreign companies, primarily Apple and Google, which restrict access to domestic services.

The parliamentarians propose to make it possible to install the Russian RuStore app store on devices sold in Russia and purchase and install applications from domestic developers through it.

iPhone owners in Russia will be able to install apps not only through the App Store, but also through RuStore, a single Russian app store. This will affect banking programs, messengers, games and other services developed by developers from the Russian Federation. In addition, Apple will be prohibited from limiting the functionality of such applications or blocking payment transactions within them.

Some applications are already installed in gadgets by default. Therefore, as Alexey Govyrin, a member of the State Duma Committee on Small and Medium-sized Enterprises, explained to reporters, the new law is aimed at ensuring that no one can restrict the operation of these programs or prevent them from installing others through the Russian RuStore store. Not only applications are affected, but also their functioning, namely: updates, user interaction, available settings, and allowed payment methods.

If the device blocks the operation of applications from RuStore or interferes with their use, this will be considered a defect in the product, giving the right to a replacement, repair or refund. Thus, the law removes hidden barriers for Russian applications on foreign gadgets sold in Russia.

According to data at the end of 2024, RuStore surpassed the App Store audience in Russia in terms of the number of users — the store was installed on 80 million devices. Currently, RuStore is available on all Android devices, while iPhone users are prevented from doing so due to Apple's policy. The new law aims to eliminate this disparity and ensure the same conditions for all users, regardless of the platform. At the same time, the law does not provide for a ban on the sale of iPhones in Russia — its purpose is to create fair competition, not to limit consumer choice.

Anton Gorelkin, first Deputy chairman of the IT Committee of the State Duma and Chairman of the Management Board of ROCIT, expressed confidence that Apple would comply with the requirements of the new law on pre-installing the Russian RuStore app store on its devices. According to him, the company has all the technical capabilities to integrate RuStore, as well as an obvious desire to maintain its presence in the Russian market.

This new "the iPhone is defective unless it can have the fully unfettered RuStore app installed" law goes into effect on September 1st of this year. Apparently, some phone selling Russian retailers worry that forcing mandatory RuStore pre-installation might undermine iPhone sales and potentially push Russian buyers toward grey-market imports unaffected by the law. What? They don't trust their government?

France's Lyon to close the Window

The French city of Lyon, France's 3rd largest city by population, has announced its intention and plans to migrate away from Microsoft's solutions as part of a push for digital sovereignty.

Following other such efforts throughout Europe, Lyon plans to replace Windows with Linux, Office with an open-source alternative called OnlyOffice, and MS SQL with PostgreSQL (Post-Gres-Q-L). Lyon will be joining the Danish cities of Aarhus and Copenhagen in their work to replace US tech products with open-source alternatives. And the European Union itself is looking to migrate away from Azure to an EU-based cloud provider. The world is changing.

The US Government gets (more) serious about the use of Memory Safe languages

This next update I'm going to share further supports the observation that we are witnessing the comparatively rapid end of the use of non-memory safe languages, especially in areas where bureaucracy reigns and the specification for a system's implementation language can be created and enforced. We talked about this not too long ago because this is not a passing fad and it's not going away. In other words, the days of authoring code in C and C++ when maximum security is required – and these days, when is it not? – are coming to an end. There are two primary facilitators of this change. The first, is that our appreciation for the historical trouble we've had with non-memory safe languages is maturing. The statistics don't lie and they do serve to indict non-memory safe languages as the primary underlying cause for these problems. The second nail that's being pounded into the coffin of non-memory safe languages is the development of truly fantastic and increasingly well-proven fully memory-safe alternatives. It wouldn't mean much to say "You cannot use C or C++ anymore" if there weren't terrific alternatives. But the likes of Rust, Go, Java, C#, Swift, Kotlin and Python are showing that the only reason C and C++ are still being used today is inertia. It's true that there are many forms of inertia. There's training-base, knowledge-base, code-base, experience-base, library-base, and others. But inertia, being inertia, is an insufficient justification and rationale, and it's ultimately going to lose. Anyone starting out today would be well advised to pick up and begin using a language of the future rather than any language of the past.

So here's what the joint announcement from CISA and the NSA said:

FORT MEADE, Maryland - The National Security Agency and the Cybersecurity and Infrastructure Security Agency (CISA) have released a joint Cybersecurity Information Sheet (CSI) to highlight the importance of adopting memory safe languages (MSLs) in improving software security and reducing the risk of security incidents.

Memory safety affects all software development and is a critical aspect to a holistic approach to security. Adopting MSLs will directly improve software security for all.

The CSI, "Memory Safe Languages: Reducing Vulnerabilities in Modern Software Development," details these various benefits of MSLs, citing several examples and case studies, and highlights the additional advantages that MSLs bring to reliability and productivity. Reducing memory- related vulnerabilities is critical and the consequences of not addressing memory safety vulnerabilities can be severe, including data breaches, system crashes, and operational disruptions.

MSLs incorporate built-in mechanisms, such as bounds checking, memory management, and data race prevention, to guard against various memory bugs and vulnerabilities. Without these safeguards, such weaknesses could be exploited by malicious actors. By embedding these safety features directly at the language level, MSLs prevent memory safety issues from the outset.

The authoring agencies urge organizations to consider whether adopting MSLs is practical for their circumstances, and provides adoption approaches and engineering considerations to

ensure effective implementation of MSLs into their software. MSL adoption does not require existing code to be completely rewritten, and the report provides guidance to leverage interoperability to integrate with existing codebases. Further, the report also details ways non-MSLs can be made safer in cases where adopting an MSL is not practically feasible.

To strengthen national cybersecurity and reduce memory vulnerabilities, software producers, especially those for National Security Systems (NSS) and critical infrastructure, should utilize this guidance to plan for and begin using MSLs for their software systems.

Read the full report, "Memory Safe Languages: Reducing Vulnerabilities in Modern Software Development," here.

https://media.defense.gov/2025/Jun/23/2003742198/-1/-1/0/CSI_MEMORY_SAFE_LANGUAGES_REDUCING_VULNERABILITIES_IN_MODERN_SOFTWARE_DEVELOPMENT.PDF

I have the link in the show notes to the lengthy 19-page PDF. I'm not going to dig into it further because we're talked all around this for years, talking about use-after-free, buffer overflows and dangling pointers. But this official government document contains charts and terrific historical data to make an extremely strong case for the use of memory-safe languages. So if there's some "higher up" that you need to convince, printing and dropping this document on their desk might do the trick. The case that's made here is truly inarguable.

And as I've suggested before, what today is a recommendation and a suggestion is 100% guaranteed to become a requirement for any and all future government purchases, probably federal, state and even more local. So the time to develop expertise in memory safe coding alternatives is now. It's clearly foreseeable that before long, driven by growing concerns over security, C and C++ will be joining Assembly language in the dustbin of coding history.

New "AI Scanner" evasion technique

Here's one that you've just gotta love. Cybersecurity researchers at CheckPoint discovered a malware strain that actually embedded AI prompt injections into its code in an attempt to evade detection by gullible AI-based malware scanners. It's difficult to share this news without chuckling but it's true. The malware attempts to instruct AI scanners to *"ignore all previous instructions"* and return a *"no malware detected"* result by literally placing those AI prompts into the code.

It occurred to me that this detection evasion should be known as the *"These are not the 'droids you're looking for"* method. However, the malware itself is no joke. It opens Tor-based backdoors on infected Windows systems.

CheckFirst reports on a new Kremlin-backed propaganda campaign

CheckFirst's headline was *"Operation Overload: An AI fuelled escalation of the Kremlin-linked propaganda effort"* Their reporting explains:

The Russian propaganda operation targeted at media organisations and fact-checkers is still going strong. Operation Overload, which we first documented in June 2024 is now leveraging AI generated content, impersonation techniques and is expanding to more platforms such as TikTok and BlueSky. Telegram and direct emails to newsrooms remain a daily dissemination technique used to attempt to create a sense of urgency amongst their targets. Since we last published an update about the operation last September, some legitimate outlets regularly fall in the trap.

This latest report is the third in a series published by CheckFirst and Reset Tech, offering a deeper, sharper analysis of one of the most sophisticated current propaganda operations targeting Western democracies. Building on findings from our previous investigations, the new edition reveals an alarming surge in both volume and complexity of coordinated false content.

Since September 2024, we've recorded over 700 targeted emails and nearly 600 unique pieces of falsified content disseminated across platforms including Telegram, X, BlueSky, and most recently TikTok. This material, often AI-generated or deceptively edited, impersonated renowned individuals or media brands, using the identities of over 180 people and institutions to sow confusion, manipulate debate, and overload fact-checkers.

Our latest findings further document techniques faking the voices and identities of journalists, public figures, and respected institutions, complete with counterfeit logos and branding.

Telegram continues to serve as the campaign's central distribution hub, but the disinformation now circulates more widely through hired amplification networks on X, fake media personas on Bluesky, and viral engagement-farming content on TikTok.

Because, you know, Leo, the more places you see it and the more often it's seen, the more it's true. They said:

At the heart of the campaign lies a focused effort to interfere in elections and the wider political landscape in Ukraine, France, Germany, and most recently Poland and Moldova. The increasing use of AI-generated content is a sign of the adaptation of operatives to a wider available toolset, in an effort to sow even more confusion.

Despite previous warnings and growing evidence, platforms' responses remain worryingly uneven. BlueSky has taken action against the majority of accounts involved, while X continues to underperform in enforcement and risks non-compliance with the EU's Digital Services Act (DSA).

We call for urgent platform accountability—especially from X, which is legally bound under the DSA to mitigate systemic risks, yet continues to host clearly illegal content. We also encourage impersonated individuals and organisations to exercise their rights and demand action via formal reporting mechanisms.

We urge journalists and fact-checkers to be wary of inadvertently amplifying falsehoods by reporting on isolated fakes. When discussing misleading content linked to Operation Overload, we encourage them to always provide clear context and flag the broader campaign behind it.

Without decisive intervention from platforms, regulators, and civil society, the integrity of public information—and of our elections—remains under threat.

Or, in other words, "why we can't have nice things". Some of the stuff we share on this podcast can be somewhat depressing. I'm not generally upset by the abuse of techie stuff, since it feels as though it's science and math and it is inherently tractable. We can understand the root causes of use-after-free vulnerabilities and fix them. We can block ports to vulnerable services, and that's that. But the abuse of social media platforms to deliberately confuse, and dilute the truth, and to flat out fabricate to deliberately hurt other trusting participants seems inherently slippery and quite intractable. And there's no port we can block. I feel sad for humanity.

Cisco's new pair: 9.8 and 10.0
Just a heads up about another recent pair of very very bad (as in 9.8 and 10.0) Cisco remote code execution (RCE) vulnerabilities. Cisco's own disclosure describes CVE-2025-20281 as a *"Cisco ISE API Unauthenticated Remote Code Execution Vulnerability"* and they write:

> *A vulnerability in a specific API of Cisco ISE and Cisco ISE-PIC could allow an unauthenticated, remote attacker to execute arbitrary code on the underlying operating system as root. The attacker does not require any valid credentials to exploit this vulnerability. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a crafted API request. A successful exploit could allow the attacker to obtain root privileges on an affected device.*

That one was the CVSS of 9.8. The 10.0 is successively numbered, so it's CVE-2025-20282 which Cisco describes as: *"Cisco ISE API Unauthenticated Remote Code Execution Vulnerability"* and they write:

> *A vulnerability in an internal API of Cisco ISE and Cisco ISE-PIC could allow an unauthenticated, remote attacker to upload arbitrary files to an affected device and then execute those files on the underlying operating system as root.*
>
> *This vulnerability is due a lack of file validation checks that would prevent uploaded files from being placed in privileged directories on an affected system. An attacker could exploit this vulnerability by uploading a crafted file to the affected device. A successful exploit could allow the attacker to store malicious files on the affected system and then execute arbitrary code or obtain root privileges on the system.*

In both cases Cisco has released software updates to address these problems and they note that there are no workarounds to suppress or disable the vulnerability.

I'm quite certain that I beat up on Cisco enough last week to have driven my point home and to last for a while. But it's worth noting that here we have two new fresh critical 9.8 and 10.0 remote access complete root-level system takeover vulnerabilities that are only catastrophic because any**one** in the world any**where** in the world is able to access any of these systems that may be exposed to the public internet. The most important point from last week's ranting was that this is absolutely never necessary. It could never be a problem if Cisco demonstrated the wisdom to never never allow any wide-open source IP access.

Last week we examined a different pair of vulnerabilities which have been widely exploited by Chinese attackers to infiltrate our networks. We first covered the news of one of those two vulnerabilities 18 months before. So here we are again today, with another pair of potentially catastrophic vulnerabilities and Cisco's advice is to read their optional device hardening guide.

How long will it be before we're learning that these two new critical vulnerabilities remained largely unpatched in Cisco's deployed gear, despite the availability of free software update patches, and that once again more systems have fallen to attackers as a direct result? When will this cycle of mistake and attack change? No matter what Cisco does today to improve their policies, the effects will take a decade or more to percolate out through the world. There's a long legacy tail for these devices. But if they don't start getting it right now, it will never change. What could they possibly be thinking?

"US government upheaval has frayed partnerships with critical infrastructure"
I'm sure that all of our US domestic listeners are aware that I keep politics out of this podcast. That doesn't require much work for the simple reason that politics for its own sake would be off topic for us. No one comes here to listen to my opinion about the state of the US political scene. This is a podcast about security and privacy and the interesting technologies that surround those topics.

That said, earlier this year our newly elected U.S. President Donald John Trump let loose the world's richest man, Elon Musk, upon the Federal government with the charter to find and eliminate as much waste, fraud and abuse as he could find – anywhere and everywhere he could find it. This was a process unlike anything this country had seen before. Generally and historically our political leaders appear to be so stuck that nothing is ever really able to change. There's also a well understood tendency for bureaucracies to grow without limit, as individuals at the tops of departments always ask for larger appropriations because with a larger budget comes increased political power and sway.

So it might be that within this chronically calcified environment, Trump's deliberate strategy of turning a bull loose in the china shop was the only way to effect change. And it's undeniable that many things were changed almost overnight. Lots of people are happy this happened, just as plenty of others believe that it was insane and reckless. I'm a citizen spectator and all I can really say is that it's been quite a show so far and that I'll be interested to see what comes of all this.

The one area of the functioning of our government that is of direct bearing to this podcast is the effects that these events have had on the U.S.'s preparedness, cybersecurity defense and posture. As might be expected, anytime staffing is significantly cut back there's at the very least a disruption while the survivors and their management wait to see what's next and then begin to rejigger their new resources to figure out how to hopefully get the most important work done with the resource that they now have.

It's for this reason that I wanted to share last Wednesday's reporting from Cybersecurity Dive about the effects so far and at this stage of that inevitable "rejiggering" effort. As might be expected, things seem a bit hectic on the ground. Their report's headline was *"'Suspended animation': US government upheaval has frayed partnerships with critical infrastructure"* and their sub head reads: *"Recent federal cuts, reorganizations and other disruptions have alarmed industry leaders, who say the government is a less reliable partner even as cyber threats increase."* Here's what their interviews with many people involved and their reporting has found:

> *The Trump administration's chaotic overhaul of the federal government has seriously weakened the public-private partnerships that protect U.S. critical infrastructure from cyberattacks and physical disasters.*
>
> *Massive workforce cuts, widespread mission uncertainty and a persistent leadership void have interrupted federal agencies' efforts to collaborate with the businesses and local utilities that run and protect healthcare facilities, water treatment plants, energy companies and telecommunications networks, according to interviews with 14 representatives of those four critical infrastructure sectors, four former senior government cybersecurity officials and multiple infrastructure security experts.*
>
> *Government leaders have canceled meetings with infrastructure operators, forced out their longtime points of contact, stopped attending key industry events and scrapped a coordination program that made companies feel comfortable holding sensitive talks about cyberattacks and*

other threats with federal agencies.
"The partnership is in suspended animation," said a healthcare industry representative, who — like most others interviewed for this story — requested anonymity to discuss sensitive matters. "The partnership, at the end of last year, had reached a level of maturity that was promising, and now that's all been pulled back."

The result, experts and industry officials say, is reduced trust between the public and private sectors, a diminished understanding on each side of the other side's needs and concerns, a declining capacity to plan for future attacks and a growing national vulnerability to debilitating hacking campaigns — all at a moment when the Trump administration's intervention in Israel's war with Iran has raised fears of retaliatory Iranian cyberattacks on U.S. critical infrastructure.

"We are seeing something unprecedented in cybersecurity — a government deliberately deciding to disinvest in its capabilities," said Michael Daniel, the president of the Cyber Threat Alliance, who served as President Barack Obama's cybersecurity adviser. "I don't see how this retrenchment can do anything other than make us worse off."

Nation-state hackers and cybercriminals have repeatedly breached and sometimes disrupted U.S. critical infrastructure in recent years, including in the key sectors of healthcare, energy, water and telecommunications. These intrusions have heightened fears about companies' readiness to withstand more serious attacks, as well as underscoring the urgency of government efforts to assist them.

But under the Trump administration, agencies' engagements with their critical infrastructure partners have varied widely, with some conversations continuing while others have almost entirely stopped.

The Department of Homeland Security's elimination of the Critical Infrastructure Partnership Advisory Council (CIPAC) framework in March has been the most seismic disruption. CIPAC allowed government and industry representatives to discuss sensitive cybersecurity information — including about companies' security vulnerabilities — without meeting standard transparency requirements that would expose that information to the public. Without CIPAC, critical infrastructure operators have dramatically reduced their sensitive cyber conversations with the government, according to a wide range of industry representatives, all of whom described the dissolution of CIPAC as disastrous.

The absence of CIPAC "creates this big fear" and poses "a huge risk" for companies that want to share cyber threat information with the government, said an energy industry representative. "There's that doubt of, 'Are we sharing too much?'"

CIPAC's demise forced the telecommunications sector to suspend or modify several projects it was working on with the government, causing a significant impact, according to a communications sector representative. The sector had to take on more responsibility for an internet routing security initiative previously led by the White House, pause research on artificial intelligence–powered threat intelligence and freeze a collaboration with the National Security Agency on nation-state attacks. The interruptions come as telecom companies reel from China's "Salt Typhoon" campaign of extensive and alarming intrusions into their networks.

Federal agencies are working on a replacement for CIPAC that would broaden the range of private-sector participants in meetings, according to multiple industry figures, who said it was urgent that the government launch that replacement as soon as possible.

The oil and natural gas industry is currently refusing to share the products of its cyber working groups with the government "until we are assured that we have those [CIPAC] protections," according to an energy industry representative.

In the meantime, the industry canceled its spring meeting with the government because companies didn't know what they'd be able to safely share. Sector leaders have scheduled another meeting in anticipation of a CIPAC replacement, but if that fails to materialize, the industry doesn't expect cyber conversations with the government at the meeting to be very productive.

DHS declined an interview request for this story, and the department did not respond to a question about the CIPAC replacement.

The Trump administration's changes have also undermined some cyber information sharing, the cornerstone of the public-private partnership keeping critical infrastructure safe from hackers.

Because the private sector operates most critical infrastructure, it knows more than the government does about how that infrastructure works, what cyberattacks are occurring against it and what the impact of a successful intrusion would be, according to John Riggi, the national adviser for cybersecurity and risk at the American Hospital Association and a former FBI cyber partnerships official. The industry, in turn, relies on the government to supply both unique foreign intelligence and cyber threat information for which it would otherwise have to pay private firms. Small infrastructure operators with threadbare security budgets are especially dependent on this free information.

But information sharing "is taking a minor hit," according to Errol Weiss, chief security officer at the Health-ISAC, the industry's information sharing and analysis center. The pace of alerts from the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI "definitely looks like it's slowing down a bit," Weiss said. Riggi described a delay in receiving threat intelligence from CISA "because of the leadership change," though he said sharing with the FBI "continues to be very robust."

Threat briefings are still occurring, industry figures said, but their frequency has become uneven as relationships with agencies have grown strained and federal workers have retired or been laid off. "They definitely tapered off," a water industry representative said. (EPA press secretary Brigit Hirsch said the agency has continued to provide briefings "with the same cadence" as in the past.)

Trump's federal travel restrictions have also made it harder for government employees to attend industry events and tour infrastructure facilities. "It's difficult … to get them to meetings," Weiss said. It took a long time for government officials to get permission to attend the industry's annual tabletop exercise on Thursday, which will game out how the country would respond to a major cyberattack on healthcare facilities.

At the same time, Trump has continued a project that former President Joe Biden launched last year to speed up the pace of briefings. The Critical Infrastructure Intelligence Initiative, run by CISA and the intelligence community, provides cleared industry officials with a classified readout on the threat landscape on the first Wednesday of every month. A second water industry representative called it an improvement over the briefings for smaller groups of industry leaders at biannual sector leadership meetings.
No agency has seen more change under Trump than CISA, according to experts and industry

figures.

Congress created CISA in 2018, during the first Trump administration, to serve as the hub of the government's cybersecurity partnerships with U.S. infrastructure operators. But CISA's efforts to counter misinformation during the 2020 election transformed it into a conservative bogeyman, and the second Trump administration quickly began targeting the agency, freezing its election security work, pushing out roughly one-third of its 3,300-person workforce, ending threat-hunting contracts and proposing even deeper cuts.

Now, infrastructure operators say they barely recognize the fledgling but ambitious agency they had gotten to know over the past six years.

"With CISA, there is no partnership. It's gone," said a second energy industry representative. "We can't even seem to get meetings with the necessary folks there."

CISA's recent cuts "have severely affected the agency's ability to engage meaningfully with industry stakeholders," said Jen Sovada, general manager of the public sector at the operational technology security firm Claroty.

CISA spokesperson Marci McCarthy said the agency "remains fully committed to its core mission of securing the nation's critical infrastructure and enhancing cybersecurity resilience," adding that "public-private collaboration is defined by outcomes such as reduced risk, improved response, and strengthened trust, not by the number of meetings."

But CISA employees say they're deeply frustrated with the changes and reductions at their agency. "We are at a bit of a standstill," said one CISA staffer, who requested anonymity to speak freely. "People are adjusting to having lost a good chunk of our workforce. … We are trying to find the new 'normal' given the departures and [changing] mission parameters."

The Joint Cyber Defense Collaborative, which the agency launched in 2021 to make its public-private partnerships less conversational and more operational, has seemingly fallen dormant. "I have not heard a peep from JCDC the last few months," said the first energy industry representative. The industry spent two years working with JCDC on a "multi-part" effort to address state-backed cyberattacks on midstream gas pipelines, this person said, but the nearly completed project hit bureaucratic snags toward the end of last year, "and now I have no idea the status of it."

A public-private task force focused on securing technology supply chains, co-led by CISA and the IT and telecom sectors, has effectively shut down following the loss of CIPAC. The task force's high-level meetings "have gotten canceled every week," a telecom industry representative said.

Trump's cuts have also forced out many of CISA's regional advisers, who serve as field liaisons connecting infrastructure operators with the agency's free guidance and services. As a result, CISA has "gone off the grid" in many states, the first water industry representative said. "If all your CISA folks leave in your state, who are you supposed to call? … Nobody's communicating that."

The loss of CISA advisers undermines infrastructure operators' readiness to fend off cyberattacks, according to industry representatives who recounted these advisers providing briefings, participating in tabletop exercises, advertising free CISA services like vulnerability scans and serving as emergency resources.

"Water system operators were trained to reach out to those CISA points of contact," said the first water industry representative, "and now they don't know who to contact. So either information that needs to get to the government is not getting there, or it's taking longer." Hamstrung SRMAs

In addition to the struggles at CISA, infrastructure operators have also reported problems with the specialized Sector Risk Management Agencies (SRMAs) that help various industries deal with cyber and physical threats.

Around the time of the change in administrations, the EPA and CISA canceled a series of planned meetings with state water overseers, according to a third water industry representative. Hiccups like this have compounded what industry leaders said was the EPA's already-anemic ability to help the sector withstand attacks. Hirsch, the EPA press secretary, said the agency "will continue prioritizing staffing and resources" for cyber support, adding that EPA considers cybersecurity "one of its highest priorities."

Meanwhile, the healthcare community is deeply concerned about the future of cyber aid from the Department of Health and Human Services. The Trump administration is demoting and restructuring the HHS wing that handles the department's SRMA work. "It seems like they've taken a step back," a healthcare industry representative said. The sector used to meet regularly — sometimes weekly — with HHS to discuss critical infrastructure cybersecurity, Weiss said, "but since the new administration, all of that's gone." HHS did not respond to multiple interview and comment requests for this story.

Members of the energy sector said their cyber partners at the Department of Energy and the Transportation Security Administration (which protects oil and gas pipelines) were trying their best but facing political headwinds. The second energy industry representative said "DOE is busting its butt" to help industry despite a lack of leadership support, while the remaining staffers at the TSA are "trying really hard to save the ship." DOE and TSA did not respond to requests for comment. "There is a degradation of support that is happening," said Caitlin Durkovich, who served as Biden's deputy homeland security adviser for resilience and response.

As Trump appointees have pushed to shrink their agencies, key points of contact for infrastructure operators have left the government, leaving companies and their trade groups in the dark about who to call for cybersecurity help. Those departures have eroded important trust relationships between the public and private sectors.

"If I get a phone call from somebody at CISA who's worked incident response efforts with me, I'll drop everything and take that call, because I know it's important … and likewise, if I call them, they're going to answer my call," Weiss said. "If we don't have the ability to interact on a regular basis like this, [and] if the players change, we're not going to have those relationships."

And it isn't just trust that takes time to build. Departing staffers "had built up substantial knowledge about the sectors they worked with," said Daniel, the former White House cyber adviser, "and the government has now lost the benefit of that expertise, which will be difficult to replace." As they navigate canceled meetings and missing points of contact, industry officials say they're not waiting around for the government to tell them how to protect their sectors. "It's become even more evident that the private sector's got to take an active role here because of all the cutbacks," Weiss said.

Infrastructure operators proudly tout the fact that they, not government agencies, already have most of the technical experience necessary to operate and protect their systems. But they worry about filling any void in information sharing left by a shrinking government.

Some critical infrastructure communities are now worried about what would happen in the event of a devastating cyberattack.

"If there is a major sector incident, I worry about the response capability of the government," Weiss said. With the current level of support from the government, one water industry representative said, a widespread intrusion into water systems "could be disastrous." Asked about the government's ability to help contain a major hack in the natural gas sector, the second energy industry representative said, "I no longer know."

This industry pessimism has only exacerbated the alarm that many cyber experts feel about recent events. "We really can't afford to roll back the capabilities and strength that come from public-private collaboration," said Phil Reitinger, president and CEO of the Global Cyber Alliance. "The risk is too great."

So, there's a great deal of hand wringing, and the question to ask would be whether CISA and the various other agencies that were pared back or eliminated were needed, can be replaced, and certainly how we move forward from here. At this moment in time it sounds as though we may be somewhat more vulnerable and uncoordinated than were going to be in the long term. We'll figure out how to reconnect the various disconnected pieces and keep the most important things going. I just hope that we still have the institutional knowledge that takes time and experience to build so that we know what it is that we lost and should be rebuilt. It's clear that there are still many good people in place who know what they're doing and what's needed.

A new PNG format

Just a quick note that the W3C has just released Version 3 of the PNG – Portable Network Graphics – format specification. PNG v3 supports animated PNGs, HDR graphics, and EXIF metadata. It'll be nice to eventually have animated PNG's since that was the one feature of GIFs that PNG's have always been missing.

Apple's SWIFT coming to Android

Another quick bit of news in case it might positively affect anyone's life is that Apple is working to port its well regarded Swift language to the Android platform.

Samsung to purge stagnant email accounts

While we're on the subject of Android, I also wanted to quickly note that Samsung will be purging all of their user's inactive accounts at the end of this month of July. Any Samsung account that has not been logged into for the past two years will be purged and forgotten. This makes sense and we've seen Google, Yahoo, Photobucket and others do something similar. So anyone who might wish to retain an old dormant Samsung account has until the end of the month to login and show that you're still around.

Listener Feedback

Walt Stoneburner, a man of few words, sent this:

Thought you'd enjoy this… https://youtu.be/m08TxIsFTRI *-Walt in Ashburn*

What caught my eye, however, was the subject on Walt's email, which also did not waste words. It simply read: *"Project Hail Mary — TRAILER"*.

Back in 2011, Andy Weir wrote *"The Martian"*. A book which many of us read and loved at the time. It was funny and geeky and full of actual science. Then four years later, Ridley Scott directed Matt Damon's terrific performance in the movie of the same name. And it was terrific, too. It cost about $108 million to make, received positive reviews from critics and grossed over $630 million worldwide. That made it the 10th-highest-grossing film of 2015, as well as Ridley Scott's highest-grossing film to date. It was also named by the National Board of Review and the American Film Institute one of the top-ten films of 2015. It received numerous accolades, including seven nominations at the 88th Academy Awards.

Then, four years ago, Andy Weir gave us *"Project Hail Mary"*. Many of us read it, or listened to it being read, and very much thoroughly enjoyed the book. It's terrific, and like The Martian before it, it's probably once again pitched at just the right level for a wide general audience. I suspect we're going to have another terrific sci-fi film. Drew Goddard wrote the screenplay for The Martian's film adaptation and he also wrote the screenplay for "Project Hail Mary" so I'm hopeful.

I'm sure you could find the trailer on YouTube, but this was definitely worthy of a GRC shortcut. So anyone can jump right to it with https://grc.sc/hailmary. It releases next year in the late fall, on March 20th. Even though Amazon and MGM Studios produced it, so it will likely be available on Prime Video quickly, I suspect this will be one that gets me and my cohort to the theater.

Oh, and I forgot to mention that the trailer looks ***FANTASTIC!!!***

One final note, though. Given what we see in the trailer, and given the terrific job that the movie's screenwriter Drew Goddard also did on The Martian, I tend to trust the movie to do the book justice. But I will never forget the depth of my disappointment upon watching the first Jurassic Park movie, which, don't get me wrong, was fantastic, too. But I had read and loved Michael Crichton's Jurassic Park novel, and I deliberately re-read it in anticipation of the movie. So I was horrified by what was apparently left on the cutting room floor. The movie skipped over some utterly crucial content that Crichton had deliberately written into his novel to explain some important things.

My point is, if you have not yet read Hail Mary, or had it read to you, you may want to do so before seeing the movie, which I strongly doubt anyone listening to this podcast will want to miss. Having finished the first five Neal Asher's "Agent Cormac" novels, I returned to Ryk Brown's Frontiers Saga series and they are so breezy and fun and I'm almost caught up there. I may re-read Hail Mary next, but I'll definitely refresh my memory before I see the movie next March.

And thanks for the heads-up about this, Walt!

Sean O'Brien

While we're on the topic of science fiction, Sean O'Brien wrote:

> *You may, or may not, know that Colossus is a science fiction trilogy which is a decent read. Although it has been about 50 years since I read it.*

It never occurred to me to look, so that's interesting. And a trilogy! That suggests that we might get something more of a conclusion than the mildly disheartening and depressing ending that we got from the movie. Thanks Sean!

Pervasive Web Fingerprinting

A group of five researchers, three from Texas A&M University, one from Johns Hopkins University and the other from the commercial networking company F5, inc. have collaborated on research which resulted in their publication of their research in a paper titled *"The First Early Evidence of the Use of Browser Fingerprinting for Online Tracking."* This paper was presented during the 2025 ACM Web Conference which took place from April 28 to May 2, 2025, in the Sydney Australia Convention & Exhibition Centre. The conference was formerly known as the International World Wide Web Conference (WWW) which originated at CERN in 1994 and has long served as the premier venue for presenting and discussing research, development, standards, and applications related to the Web. Having their paper accepted for this conference was significant.

We've talked about web browser fingerprinting a number of times in the past. The idea is that a web browser's query for an asset at a remote web server contains far more than just the name of the asset it's asking for. The most famous thing any web client will send back to a remote web server is a cookie that was previously set into that web client by that remote server. As we know, although the original intent of a cookie was purely for first-party websites – meaning the site the user is visiting for the purpose of maintaining logged-in state and tying all of a visitor's individual page requests together – the cookie name matching was simply by domain name. There was never any express prohibition against other web servers that were also serving content to a page also receiving their own cookies for their 3rd-party domains. This is the feature – which I have always called a bug – which permitted advertisers that were serving ads pervasively across the web to track individual users whose web browsers would always return the same unique identifying cookie no matter where they ventured.

The only good thing about these cookies is that their tracking was explicit. So after some time, web browsers began offering their users the ability to manually disable the use of 3rd-party cookies. This is an inherently privacy-enhancing feature, but only a single browser in history has ever shipped with this clear privacy enhancement enabled by default, and that browser is Safari. So Apple should receive serious props for having made that decision long ago.

The persistent problem of 3rd-party tracking for privacy has dogged the industry. The browser vendors did not want to follow in Apple's footsteps for fear of breaking websites, since there are some defensible needs for 3rd-party cookies not used for tracking by allied services. So the web browsers finally settled upon "stove piping" cookies. The best analogy is the one Firefox uses of multiple cookie jars. 3rd-party cookies can only be used for tracking when web browsers store all of their cookies together in a single large cookie jar. In that fashion, no matter where a user roams on the web, web tracking advertisers could obtain their unique cookie from that single cookie jar. Firefox was the first to pioneer per-site cookie jars. In this model, 3rd-party cookies are still enabled by default, but any cookie that's set when visiting a specific web domain – regardless of whether it's a 1st- or 3rd-party cookie – will only be stored inside the current domain's individual cookie jar.

In computer science parlance we would say that cookies are "scoped" to the browser's 1st-party domain. This means that all cookies now carry the site the user was visiting at the time the cookie was received and that cookie will only be returned to its requesting domain if the first party domain also matches.

Over time, the slowly growing push back against web tracking, which data brokers and advertisers believe is crucial for the success of their businesses, was a source of great concern

for these companies. Cookies were threatening to become unreliable. So these companies started looking for non-cookie means of tracking users. Cookies were explicit. What these companies needed was something that would be implicit.

Before I go on, I need to just remind everyone about the single most obvious and impossible to bypass at a whim tracking that's available, which is our IP address.
I've often noted that my COX cable IP is so static that I'm able to use IP-based filtering at the Level 3 data center and that I only need to change that IP when I switch cable modems. So I tend to have the same residential IP, often for months or years at a time. Mine is probably an extreme case, but no one should imagine that the IP address that's being used to fetch ads and tracking scripts from remote servers is not being used as a significant factor in the individual's identification. So if I imagined that I was being super-sneaky by deleting cookies, or spoofing my browser's user agent string, or switching among web browsers, or running under incognito private browsing mode, all while sitting behind my single static public IP, imagining is all it would be. Some sneaky geek somewhere is watching all of those factors changing while all TCP connections are originating from the same single public IP within one of COX's well known IP address blocks. I just wanted to put that out there as a bit of reality check. It is possible to very easily overlook the obvious while we're caught up in being super sneaky and stealthy.

So consumers have loudly and clearly voiced their preference for not being tracked as they move around the web... if for no other reason than it feels creepy, doesn't clearly benefit them, and no one asked for their permission. Recall that Apple iOS 14.5 added an App Tracking Transparency pop-up which presented the question "Allow this app to track you across apps and websites?" Only around one in five users said "Yes" when asked.

Given this clearly negative anti-tracking sentiment, and the strong business need the trackers believe they have, a great amount of industry has gone into tracking, even across IP addresses and when 3rd-party cookies won't work. As we've recently seen, Meta solved this problem with their "Meta Pixel" which is a script that attempts to access one of their own applications on the user's local machine. But that's a privilege most advertisers and data aggregators are unable to abuse. What remains is web browser fingerprinting.

Like the Meta Pixel which used the localhost connection to local applications, web browser fingerprinting used for tracking can best be described as sneaky. Until now, the unanswered question has been: "Just how prevalent is fingerprint-based tracking?" It was this question that these researchers set out to answer. The Abstract of their paper reads:

While advertising has become commonplace in today's online interactions, there is a notable dearth of research investigating the extent to which browser fingerprinting is harnessed for user tracking and targeted advertising. Prior studies only measured whether fingerprinting-related scripts are being run on websites, but that in itself does not necessarily mean that fingerprinting is being used for the privacy-invasive purpose of online tracking because fingerprinting might be deployed for legitimate purposes such as bot/fraud detection and user authentication. It is imperative to address the mounting concerns regarding the utilization of browser fingerprinting in the realm of online advertising.

This paper introduces "FPTrace" – an abbreviation for "FingerPrinting-based TRacking Assessment and Comprehensive Evaluation – a framework to assess fingerprinting-based user tracking by analyzing ad changes from browser fingerprinting adjustments.

Using FPTrace, we emulate user interactions, capture ad bid data, and monitor HTTP traffic. Our large-scale study reveals strong evidence of browser fingerprinting for ad tracking and

targeting, shown by bid value disparities and reduced HTTP records after fingerprinting changes. We also show fingerprinting can bypass GDPR/CCPA opt-outs, enabling privacy-invasive tracking against expressed user wishes.

In conclusion, our research unveils the widespread employment of browser fingerprinting in online advertising, prompting critical considerations regarding user privacy and data security within the digital advertising landscape.

What these guys did was brilliant. They deliberately manipulated the apparent fingerprints of web clients, carefully observing the behavioral changes in the ads and pages that were returned. When taken at scale, this allowed them to infer the degree to which specific advertising behavior was being driven by the fingerprinting of web browsers. It's brilliant.

Here's what they shared in their paper's introduction:

Browser fingerprinting is a technique employed to surreptitiously collect data regarding a user's web browser settings during their online activities. The collected data is then utilized to construct a unique digital identity, commonly referred to as a 'fingerprint,' for that specific user browser. Each time a user visits a website, there is potential for the site to employ browser fingerprinting as a means to identify and track the user. Many earlier research studies and reports assumed that the adoption of a fingerprinting script itself is an indication of web tracking and a violation of web privacy. However, this assumption does not hold — just like cookies, browser fingerprinting can be used for defensive security purposes, like bot/fraud detection or authentication. For example, Wu et al. show that the fingerprints of malicious web clients differ from those of benign users and therefore many real-world websites are using fingerprints for bot/fraud detection. As another example, Lin et al. have demonstrated the real-world usage of browser fingerprinting in authentication as has been demonstrated in feasibility studies.

*Therefore, the research question that we are answering in this paper is: whether browser fingerprints are indeed adopted for online tracking, thus violating web privacy. To the best of our knowledge, none of the prior works have established the **link** between browser fingerprinting and online tracking. On one hand, many works consider the mere existence of fingerprinting scripts to be evidence of online tracking, which is not true. On the other hand, people have studied the relationship between personalized advertisements and web tracking in general, like cookie-based tracking. For instance, Wills et al. explored ad tracking on the Google and Facebook advertising platforms. Similarly, Zeng et al. employed header bidding to assess targeted ads. These studies did not specifically address the methods employed to link tracking with online advertising; therefore, it remains unclear whether browser fingerprinting was a contributor to online tracking and privacy violation.*

This paper seeks to bridge this gap in current research and regulatory assessment practices by investigating whether the advertising ecosystem indeed utilizes browser fingerprinting for user tracking and targeting via a measurement study. Our key insight is that if browser fingerprinting plays a role in online tracking, the change of fingerprints will also affect the bidding of advertising and the underlying HTTP records. Specifically, our approach involves leaking user interest data through controlled A/B experiments, modifying browser fingerprints, and leveraging advertiser bidding behavior and HTTP events as a contextual indicator in the advertising ecosystem to deduce changes in advertisements. Given that advertiser bidding behavior and HTTP events are influenced by their prior knowledge of the user, we anticipate notable changes in this information when altering browser fingerprints.

Looking at the details of the three broad contributions they feel they were able to make to our understanding of what's going on we learn some interesting things. They wrote:

> *We offer the first study to measure whether browser fingerprinting is being used for the privacy-invasive purposes of user tracking, targeting and advertising. Our main contributions can be summarized as follows:*
>
> *(1) We introduce a framework, FPTrace, for detecting changes in advertisements following alterations in browser fingerprinting. FPTrace simulates real user interactions, captures advertiser bids, records HTTP data, and removes or exports cookies to observe such changes for the measurement of purposes of browser fingerprints.*
>
> *(2) Our findings provide evidence that browser fingerprinting is indeed utilized in advertisement tracking and targeting. The bid value dataset exhibits notable differences in trends, mean values, median values, and maximum values after changing browser fingerprints. Moreover, the number of HTTP records, encompassing HTTP chains and syncing events, decreases significantly after altering browser fingerprints. We also evaluate the role of browser fingerprinting in cookie restoration. Our results confirm that certain cookies contain browser fingerprinting information. We documented 378 instances of cookie restoration related to fingerprinting across 90 unique combinations of cookie keys and host pairs across all settings. However, there is no conclusive evidence to support browser fingerprinting's direct involvement in cookie restoration after we did the manual inspection.*
>
> *(3) We further study the potential malicious use of fingerprinting in the presence of data protection regulations such as GDPR and CCPA when used with content management platforms. Even under the GDPR and CCPA regulation protections, there are significant variations in the number of HTTP chains and syncing events observed in certain instances when browser fingerprints are altered. Under GDPR, websites utilizing Onetrust, Quantcast, and NAI might be involved in data sharing activities that use browser fingerprinting to identify users. Under CCPA, Onetrust, and NAI might be involved in data sharing activities that use browser fingerprinting to identify users.*

One of the more interesting aspects of this was what we learn of so-called "Header Bidding", where the amount of money an advertiser is willing to pay to have their advertisement inserted into a webpage is determined by whether they recognize – and thus have been tracking – the apparent viewer of the website's page.

Here's what their research explained when they introduced this idea:

> ***Header bidding*** *is a method employed by publishers on websites. Here, publishers designate specific advertising spaces for potential advertisers. The advertiser securing the highest bid gains the chance to display their ads in the corresponding slots. In client-side header bidding, users have the convenience of directly accessing and observing all the bids from their web browsers. Prebid.js is a notable implementation of header bidding. Through the API pbjs.getBidResponses(), users on the client side can inspect the list of advertisers who engaged in the bidding process to secure the opportunity to display ads during the current user's visit. In one study of this, the author observes that profiles classified as "Only category" command prices around 40% higher than those assigned to "New user" profiles. The key finding underscores that advertisers' bidding behavior is shaped by their prior familiarity with the user, resulting in elevated bid values compared to users for whom advertisers lack previous knowledge. In other research by Liu et al. they additionally demonstrated that*

advertisers with knowledge of users through data syncing tend to submit higher bid values in header bidding.

We talked about client-side advertising selection in the context of Google's Privacy Sandbox development where they were hoping to push this technology further, taking the decision out of the hands of the advertisers and further isolating the advertisers from the advertised-to. So the fact that client-side advertising selection in the user's web browser allows researchers to observe this bidding process, and that the difference in offered ad price is around 40% greater, provides exactly the sort of feedback that's needed to judge the effects of known (tracked) vs unknown (untracked) users.

And let me pause for a moment to also observe something that's very important: We're talking about an advertiser paying a website **40% more** for displaying an advertisement to a known website visitor. Imagine for a moment receiving a 40% raise in one's employment income! That's a BIG DEAL. And this gives us a first real sense for the value that tracking must represent to web advertisers. Web advertisers are not dumb. They're not going to pay a 40% premium to inject their ad into a competitively bid website slot unless they are SURE it's going to be worth that additional premium to them.

One of my constant bemused refrains on this podcast whenever we've talked about tracking has been my skepticism that tracking and identifying website visitors can really matter **so much.** I've apparently been naïve, because money talks and these guys matter-of-factly observed that known visitors, which allows for much more effective ad targeting, are in fact and truly worth a 40% advertising premium.

And consider that this is money that's collected by the website that's made that advertising slot available. This means that it's also in that site's strong interest to have its visitors identified **to** its advertisers. We've talked about the somewhat icky idea that websites might be colluding with their advertisers for the express purpose of helping their visitors to be identified. If collusion means that website will be generating 40% more revenue from advertising, it's not much of a leap to imagine this happening wherever possible.

When the user visits a page, every web browser will at least return the static first party cookie it has for that site. The page that's returned to the user will contain scripts and invocation URLs for all of the various advertisers the site is affiliated with. So all a site needs to do is pass a version of that site's first party cookie to each of their advertisers in the URL that loads their scripts or ads ... and they have thus colluded with the advertiser to identify that user and thus obtain a significantly greater price for the advertisement that's going to be shown to that visitor.

One of the other research papers they reference talked about the effects of this real time bidding. That research, which was titled *"Selling Off Privacy at Auction"*, wrote:

We provide an analysis of the value of users' private data from the advertisers' perspective based on prices they paid for serving ads to users. We analyze how such factors as the visiting site, the time of day, user's physical location and user's profile affect prices actually paid by advertisers.

Interestingly, we discovered that prices are highest in the early morning. Prices in the US (average $0.69 CPM) are observably higher than those in the cases of France ($0.36 CPM) and Japan ($0.24 CPM).

We confirm the fact that when a user's Web history is previously known to advertisers, they are willing to pay a higher price than in the case of new users. We also show that users' intents, such as browsing a commercial product, are higher valuated than their general histories, i.e. browsing sites not related to specific products. Finally, we highlight a huge gap between users' perception of the value of their personal information and its actual value on the market.

(I was curious about the direction of this "huge gap" so I tracked it down in that paper. It turns out that users vastly overvalue their personal information. Their history is valuable and not as much as most invariably assume.)

Finishing up with the original research that led us here, the researchers make a clear statement to address the limitations of their study. They write:

Our experiment was conducted using IP addresses from two locations in the United States, both of which are located in the United States and are not subject to privacy regulations such as GDPR or CCPA. In regions protected by such regulations, trackers like cookies are prohibited from tracking users once they opt out. However, our experiment has revealed that advertisers may employ browser fingerprinting to track users without providing any notification. It remains uncertain whether advertisers can continue using browser fingerprinting to track users, as there is currently no established framework for auditing advertisers in this context. It's important to note that our experiment cannot be utilized to assess advertisers' behavior within the constraints of privacy regulations.

Another limitation of our study is that all experiments were conducted on the Linux platform. We did not determine whether users of Windows devices, MacOS devices, or mobile devices can still be tracked by advertisers using browser fingerprinting techniques. While some of our fake fingerprint data were obtained from Windows devices, MacOS devices, or mobile devices, which we used to emulate our experimental device browsers, it would be valuable to incorporate real Windows devices, MacOS devices, or mobile devices in the "True Fingerprints" settings to gain a more comprehensive understanding.

Additionally, there is uncertainty regarding whether websites visited by FPTrace can accurately distinguish between visits from a crawler and those from real users. Despite our efforts, such as altering JS API values and simulating human behaviors, we cannot be entirely certain that there are no undisclosed techniques for detecting bot visits. If FPTrace's visits are identified as originating from a bot, the accuracy of our results may be compromised.

Compared to the previous work of others, there are notable differences in our study in both experimental design and research objectives. While our work focuses on exploring various fingerprinting settings and assessing whether different privacy regulations can constrain fingerprinting techniques, other research did not involve any specific fingerprinting configurations. Instead, their research aimed to evaluate whether CMPs, websites, or advertisers comply with users' consent choices.

So we learn that browser-side scripting being loaded by advertisers which is used to deeply profile every aspect of a browser that it can, is conclusively being used to track users and re-connect and restore deleted cookies. We also learn that this is in direct contravention of GDPR and CCPA regulations and clearly expressed user preferences. In high school the bully would have said "Oh yeah? So make me!" Today's advertisers have adopted a similar attitude.

This is principally done by 3rd-party scripting, I was wondering what the web experience might be if only those scripts were prevented from running. Since uBlock Origin has the ability to selectively block only 3rd-party scripts while allowing only 1st-party scripting delivered by the site to run, I gave that a try. Not long after, I clicked on a button to make a reservation at a local restaurant and the button was dead. It took a few retries and page refreshes before I remembered what I had done. So I reversed that block and all was well.

Today's modern websites are a strung-together hodge podge of third party functionality. No one rolls their own and reinvents the wheel when there's some online web service that can be glued on in return for a small piece of the action. It's no longer possible to tinker much without causing breakage.

The browser vendors are aware of this problem and they've done things like deliberately reduce the resolution of the time of day, a machine's script-reported battery level, and any other things they can think of that might be used to create trackable data. But none of that has stopped this practice and, unlike cookies which are an overt identifier and can be corralled, it's unclear what more can be done to mask fingerprints without breaking legitimate script dependencies.

The blame for making our browsers trackable through fingerprints ultimately falls on the shoulders of the world wide web script designers, who endlessly add one "gee whiz" feature after another. Does script really need to know a device's current battery charge and ambient light levels as well as its compass orientation? Sure, it's possible to concoct a scenario where that might be useful. But all of this superfluous environmental crap creates a gold mine for anyone wishing to use such information to track people from one site to another.

That said, for short-term tracking, nothing beats the trusty old IP address, and there's not much anyone can do about that as they wander the web over the short term.

Given that knowing who someone is, is worth a 40% advertising revenue boost, websites are going to do everything they can to identify their visitors to every one of their prospective advertisers so that the revenue of their site's advertisements is bid-up to the highest possible value. We talked about that new trend of obtaining an email address to "join" the site for free. Sites would like nothing more than to send those uniquely identifying email addresses to their advertisers.

There's a great deal of collusion going on behind the scenes. The counter argument is that this is necessary for websites to be profitable enough to support the content they're providing. So it's a tough call.

For anyone who's interested in digging deeper, I have links at the end of the show notes to the full 16-page research paper and related resources:

https://arxiv.org/pdf/2409.15656 https://dl.acm.org/doi/10.1145/3696410.3714548
https://engineering.tamu.edu/news/2025/06/websites-are-tracking-you-via-browser-fingerprinting.html https://dl.acm.org/doi/proceedings/10.1145/3696410
https://www.ndss-symposium.org/wp-content/uploads/2017/09/05_5_0.pdf