

Security Now! #953 - 12-19-23

"Active Listening"

This week on Security Now!

Is the U.S. ever going to be able to introduce new child protection legislation or are we going to continue punting to the U.S. constitution? 2024 means the beginning of the end of traditional 3rd-party cookies in Chrome. What's the plan for that? How much did the Internet grow during 2023? and why? What's the most used browser-based query language? What's the updated ranking of sites by popularity? What percentage of total Internet traffic is generated by automation? Those and many other interesting stats have been shared by Cloudflare. Then, after catching up with a bit of SpinRite news and some feedback from our listeners, we're going to examine the content of some very disturbing webpages that Cox Media Group originally posted then quickly removed.

Schrödinger's Bowls currently exist in a state of being both broken and unbroken... until the cupboard is opened to determine their fate.



Security News

Meta vs the FTC

Meta is suing the U.S. Federal Trade Commission on the grounds that it – the FTC – does not have the constitutional authority to hold Meta accountable and it **\$200 billion dollars** for Meta's deliberate and flagrant violation of the Children's Online Privacy Protection Act (COPPA), which requires parents to sign off before websites gather and use personal information from children younger than 13. The FTC claims that the recent lawsuit filed by 41 states' attorneys general documents that Meta had knowledge that millions of users younger than 13 use its services.

The thing that caught my eye about this is that unbiased observers believe that Meta's argument **likely has merit** and that the U.S. Supreme Court may side with Meta if the dispute reaches that highest court. This is another of those issues (and they're piling up) where what's really needed is for U.S. lawmakers in Congress to make some laws, in lieu of continuing to over leverage and over interpret the U.S. Constitution. Not surprisingly, the U.S. Constitution, largely written in 1787 – before two paper cups connected by a string was invented – offers little guidance on the issue of age-based IP-driven website content filtering. What we need are some laws here.

But that turns out to be a problem, too. We've spent some time looking at the UK's attempt to force some means of monitoring all encrypted messaging. And the future of the EU's legislation to force browsers to accept their countries' individual certificate authorities without question remains unclear. The clear pattern here is that technology rarely seems to line up with what lawmakers want. Unfortunately, that never appears to deter them or to make them want it less; they just become more insistent that they ought to be able to have anything they want.

Along those lines, we have a mess brewing here in the U.S. that Meta's pushback against the FTC brings back into focus. It promises to create another challenge that technology may not be able to deliver, and this happens every time we ask the Internet's amazing array of technologies to do something it was never designed to do: Legislators are talking about wanting Internet content providers to protect young people in the U.S. by blocking content based on age. And even if that was all they wanted, it's unclear how technology could provide that. But there are other legislators who believe that some young people must continue to have unfettered access to content that's inherently controversial. So we can't even agree on what we want, even if the Internet could provide it.

Suzanne Smalley, a reporter for The Record, has been following this developing story. Her most recent installment last Monday covered Meta's pushback against the FTC, which may actually lack the legal grounds for their attempted regulation of Meta. But back in July, Suzanne posted a piece in The Record which captured the heart of the issue. Under the headline "*Sweeping and controversial children's digital privacy bills head to full Senate*", after my light editing for the podcast, Suzanne wrote this:

Two bills designed to bolster children's privacy and safety online advanced in the Senate on Thursday [again, that's a Thursday back in July] after months of infighting between children's advocacy organizations and technology civil rights groups over what the latter see as problematic freedom of speech and privacy concerns in the legislation.

Despite the mixed views, the Commerce, Science and Transportation Committee voted to advance the bills, known as the Kids Online Safety Act (KOSA) and the Children and Teens Online Privacy Protection Act (COPPA 2.0). The latter updates an original COPPA bill passed in 1998, which is considered the first and only major federal privacy legislation.

Committee Chair Sen. Maria Cantwell (D-WA) cheered both bills' success, saying of COPPA 2.0 that children and teens can be "overwhelmed with the complexities of online content that is manipulated and targeted at them." She said the bill strengthens protections and closes loopholes while ensuring data of children under age 17 is protected more rigorously.

President Joe Biden, who discussed the need for stricter children's privacy laws in his State of the Union address, urged the committee to approve the bills earlier this week, but there are questions about their potential to become law, particularly since there are no House versions.

COPPA 2.0 changes the existing law to require online services to stop collecting data from kids under age 17 (raised from under age 13). KOSA is far more sweeping and requires platforms to filter content directed to users under age 17 in the name of preventing, for example, suicide and anorexia.

While celebrating the progress of KOSA, Cantwell acknowledged the profound concerns in the free speech and technology civil rights communities about how the bill would block vital LGBTQ content from older teens. Acknowledging the advocates' concerns, Cantwell said, "we will continue to work with them."

KOSA, the more politically charged of the two bills, is supported by a range of children's privacy groups and larger organizations devoted to childrens' mental health, including Common Sense Media, the American Psychological Association, Fairplay and the American Academy of Pediatrics.

A letter to senators signed by more than 200 groups pointed to troubling statistics that advocates say are directly tied to the broad freedom of access children have to online content and the uncontrolled and often profit-driven behavior of companies pumping it out to them.

The letter highlighted that depression rates in teens doubled from 2009 to 2019 and cited a similar doubling of eating disorder emergency room admissions for teen girls from 2019 to now.

More than 90,000 pro-eating disorder accounts with 20 million followers appear on Instagram, the letter said, with Meta earning an estimated \$230 million annually from such accounts. The letter signed by more than 200 groups said: "After numerous hearings and abundant research findings, the evidence is clear of the potential harms social media platforms can have on the brain development and mental health of our nation's youth, including hazardous substance use, eating disorders, and self-harm."

The founder and CEO of Common Sense Media, which focuses on children's privacy and safety online, echoed the letter's assertions Thursday and highlighted the outdatedness of current laws governing children's use of technology, saying the bipartisan group of sponsors were "doing their part to bring tech policy into the 21st century."

A large number of freedom of expression and data privacy groups, including the Electronic Frontier Foundation, the Center for Democracy and Technology (CDT) and the ACLU, have lobbied hard **against** KOSA in particular, saying the costs it imposes to address children's online safety are too high.

KOSA would mandate parental consent when children under age 13 create online accounts and require providers to give the parents of these children the ability to change privacy settings. As a result, advocates say, children will be forced to tell their parents which sites they visit.

They point to the bill's inclusion of a so-called duty of care provision, which they say creates an obligation for online service providers to prevent harms to minors under age 17. But in doing so, the bill's broad language will effectively block a wide range of important information, including about mental and reproductive health, LGBTQ issues, and substance use dependency support, they say. The requirement to "prevent" harm is extreme, advocates say, and will lead to extensive and often ineffective content filtering.

The bill also will likely trigger an overreaction from online content providers who Emma Llansó, director of the free expression project at CDT, said will block far more content than necessary over liability concerns. Llansó also criticized how the bill would give civil enforcement power to uphold the law to states' attorney generals, many of whom she said have extreme views on reproductive care and LGBTQ rights. At a time when many states are already seeking to block information about gender affirming and reproductive health care, she said, the bill "puts the most vulnerable young people at a serious disadvantage, facing harassment and consistent targeting of their speech or the speech of people who might be resources or lifelines for them."

KOSA inserts itself into the parent-child relationship while ignoring minors' privacy, constitutional and human rights access to information, according to Cody Venzke, who is senior policy counsel for surveillance, privacy, and technology at the ACLU. Venzke said: "KOSA has created a blunt technological veto over minors' right to learn, explore, and speak."

Advocates also have argued that age verification requirements in both bills would undermine adult and children's privacy. In a recent blog post a CDT policy analyst wrote that because KOSA proposes having online services "limit by default" minors' ability to communicate with other users — a provision that can't realistically be applied to adults — it will be impossible to separate adults and children without asking for identification, which could include birth certificates or even facial scans.

The large number of children's health organizations pushing KOSA say years of failure by social media companies to protect children and adolescents from harmful effects is what prompted the bill's "duty of care." The bill's provision for substantial parental controls will create a far safer digital environment, they say.

Citing the 90,000 Instagram accounts promoting eating disorders, the Common Sense Media's Technology Policy Counsel said currently many platforms are sitting idly by continuing to "profit off of a bubble like that." The Counsel acknowledged that content filtering isn't perfect, but said KOSA can be refined over time. In the meantime, she said, under the new law policymakers will learn more about how online providers' algorithms work, which they can leverage to better protect kids.

Meanwhile, over on the COPPA 2.0 side, many advocates worry the COPPA 2.0 bill would undermine privacy for substantially more people because it will be less clear who is a child when data collection bans apply to users as old as 16. As a result, age verification will be

required from a larger number of people, they say.

With users under age 13, content filtering is easier to do. But 16-year-olds use most of the Internet making age verification much more sweeping and problematic.

Eric Null, who is co-director of the privacy and data project at CDT, said, as with KOSA, COPPA 2.0's imposition of an implicit society-wide need for identification could quite possibly lead to platforms requiring photos of all users' faces. The CDT blog says the bill is poorly designed, pointing to how the bill's "verifiable parental consent mechanisms" in some cases allow any adult to provide consent, which would make the law easy to circumvent and meaningless. Null said, "A big issue from our perspective is that when you raise that age limit, the number of websites that have to verify the age of all their users skyrockets."

So the UK and the EU are certainly not alone in facing challenges created by the Internet. Here in the U.S., what I just shared clarifies **why** we don't have legislation around this. It's not for any lack of recognition that problems exist. The problem is that there's zero consensus about what the problem is. Half of our legislators and action groups want to protect children from content **they** consider to be harmful, while the other half feels – just as strongly – that those same children need protected private access to exactly that same controversial information for their benefit.

The way things are currently balanced in Congress, I don't think we need to worry about anything happening in the way of new legislation anytime soon. It should be clear to everyone why Congress is deadlocked over this legislation. And as I noted earlier, Suzanne's updated reporting suggests that the FTC may have broadly overreached and overstepped and that Meta, whose size certainly enables it to defend itself, may prevail in the FTC's attempts to rein in its behavior with lawsuits and stunning monetary fines. \$200 billion dollars is money worth fighting over.

Google / Chrome to begin deprecating the use of 3rd-party cookies

The recent developer blog discussing the release of Chrome 120 included a little blurb that reminded me that it's about to be 2024. The blog wrote:

- *And a reminder that Chrome is working towards deprecating third party cookies. In January [meaning, two weeks from now!] an experiment begins that could affect your website, so it's important that you check.*

And they provide a link to an article: "*Preparing for the end of third-party cookies for auditing and mitigating steps.*" On that page they note:

If your site uses third-party cookies it's time to take action as we approach their deprecation. Chrome plans to disable third-party cookies for 1% of users starting in Q1 of 2024 to facilitate testing, and then ramp up to 100% of users by Q3 2024. The ramp up to 100% of users is subject to addressing any remaining competition concerns of the UK's Competition and Markets Authority (CMA).

What Google is referring to here is that it appears that the UK government's Competition and Markets Authority has expressed some concern on behalf of UK advertisers that they might be materially damaged by Google's removal of 3rd-party tracking cookies from Chrome. Oh, gee. So this appears to be the sort of nonsense that any global technology behemoth such as Google just needs to put up with as part of doing business. Google's posting continues:

Our goal with the Privacy Sandbox is to reduce cross-site tracking while still enabling the functionality that keeps online content and services freely accessible by everyone. Deprecating and removing third-party cookies encapsulates the challenge, as they enable critical functionality across sign-in, fraud protection, advertising, and generally the ability to embed rich, third-party content in your sites—but at the same time they're also the key enablers of cross-site tracking.

In our previous major milestone, we launched a range of APIs providing a privacy-focused alternative to today's status quo for use cases like identity, advertising, and fraud detection. With alternatives in place, we can now move on to begin phasing out third-party cookies.

As we know, Google's replacement which will allow advertisers to obtain some weak "interest" categories about visitors is TOPICS. We've talked about it here several times and it's a very nice solution.

So 2024 will finally be the year when 3rd-party cookie behavior is changed for the better. It won't be that a 3rd-party site cannot still place a cookie into a user's browser. They can. But that same 3rd-party site will not be able to retrieve that same cookie when that visitor is at any other site. This is a huge behavior change. Firefox led the way with this more than two years ago when with Firefox 86 in February of 2021 they introduced "Total Cookie Protection." Back then it was present but not enabled by default. Two years later, in April of this year, it went live and was enabled by default. And, gee... the world as we know it didn't end.

All that happened was the addition of cookie storage partitioning: Historically, all web browsers maintained a single global cookie jar which held all cookies being stored by the browser. This was the single fact which made tracking possible since any advertiser offering content to multiple websites would receive their same "tracking" cookie no matter where the user traveled. But with the adoption of Firefox's Total Cookie Protection, each website effectively gets its own private cookie jar which stores any cookies that anyone wants to set while the user is at that site. But once the user changes to any other site, **that** site's cookie jar becomes current. So while advertisers are still welcome to set their cookies at every site, all cookie linkage between sites is broken.

Google certainly already knows that catching Chrome up with Firefox in this regard won't end the Internet. But there's no arguing that this really does represent a significant change to the way browsers have ever worked by default. So it's reasonable for Chrome to be sticking a toe in the water, before jumping in headlong.

We know that change often needs to be forced. So this is Chrome saying: *"Hey, we're not kidding about this. This change is coming, so you need to make sure that this isn't going to be breaking anything weird you might be doing."*

Cloudflare's look back at 2023

The last piece of news I want to share before we get to SpinRite and some feedback is Cloudflare's summary of interesting statistics from 2023. This is Cloudflare's 4th annual review of Internet trends and patterns observed throughout the year at both a global and a country/region level for a variety of metrics.

- Global Internet traffic grew 25%. They noted that major holidays, severe weather, and intentional shutdowns clearly impacted Internet traffic. Remember all that dark fiber we once had during that Internet over-build? I'd bet there's far less excess today than there once was. But think about that for a minute: 25% growth in Internet traffic in one year. That's a massive increase in something that's already as mature as the Internet. The only thing I can imagine that might account for that is the continuing increase in the use of streaming media for content delivery. I had been a happy TiVo user for years. Switching from Analog to Digital but remaining with traditional cable TV. Then, six years ago when I was setting up my home with Lorrie, I tried an experiment. We never asked Cox for cable TV – only Internet service. And I've never looked back.
- Not surprisingly, Google was again the most popular general Internet service, but TikTok, which was the leader two years ago in 2021, fell to fourth place. The ranking among the top 10, from #1 to #10 is: Google, Facebook, Apple, TikTok, Microsoft, YouTube, AWS, Instagram, Amazon and iCloud. I'm a bit surprised that Apple's domain is in the #3 position, above TikTok in #4, YouTube at #6 and Instagram at #8.
- OpenAI was the most popular service in the emerging Generative AI category, and Binance remained the most popular Cryptocurrency service.
- On the mobile front, also no surprise, over two-thirds of all mobile device traffic was consumed by Android devices with Android commanding a >90% share of mobile device traffic in over 25 countries/regions.
- In the skies above us, the global traffic from Starlink nearly tripled in 2023. After initiating service in Brazil in mid-2022, Starlink traffic from that country jumped by more than a factor of 17x in 2023.
- On websites, Google Analytics, React, and HubSpot were among the most popular technologies.
- Worldwide, nearly half of web requests now use HTTP/2, with 20% using HTTP/3.
- NodeJS was the most popular language used for making automated API requests. Cloudflare noted that as developers increasingly use automated API calls to power dynamic websites and applications, they're able to use their visibility into Web traffic, since they are often serving as a proxy in front of web services, to identify the languages the API clients are written in. So, beyond NodeJS holding the #1 spot at 14.6%, the ranking in decreasing order behind NodeJS is Go at 8.4%, Java at 7%, Python at 6.8% and .NET at 4.3%.
- And during 2023, Googlebot was responsible for the highest volume of request traffic to

Cloudflare's hosted and proxied sites.

As for Internet connectivity & Speed...

- Over 180 Internet outages were observed around the world in 2023, with many deliberately created by government-directed regional and national shutdowns of their own Internet connectivity.
- Only one third of IPv6-capable requests worldwide were made over IPv6. So even though IPv6-capable servers are still rare, among those services that do support IPv6, two thirds of the queries they received were to their IPv4 addresses.
- The top 10 countries all had measured average download speeds above 200 Mbps, with Iceland showing the best results across all four measured Internet quality metrics. The reason for Iceland's outstanding performance is that over 85% of all Internet connections are over fiber.
- Over 40% of all global traffic is exchanged with mobile devices and in more than 80 countries and regions, the **majority** of all traffic is exchanged with mobile devices.

And on the security front:

- Just under 6% of global traffic was mitigated by Cloudflare's systems as being potentially malicious or for customer-defined reasons. In the United States, 3.65% of traffic was mitigated, while in South Korea, it was 8.36%.
- A third of global bot traffic comes from the United States, and over 11% of global bot traffic comes from Amazon Web Services. And they don't "bots" as in mean malicious bots. Cloudflare means anything that's automated. So any and all legitimate Internet-indexing bots would doubtless be a hefty part of that.
- But on the malicious front, globally, Finance was the most attacked industry, but the timing of spikes in mitigated traffic and the target industries varied widely throughout the year and around the world. So it's not all just where the money is.
- Even though the two year old Log4J vulnerability remained a top target for attacks during 2023, the HTTP/2 Rapid Reset attacks, which we covered a few months back, emerged as a significant new vulnerability, beginning with a flurry of record-breaking attacks.
- And get this!: 1.7% of TLS 1.3 traffic is already using post-quantum encryption!
- In malicious eMail messages, deceptive links (in other words, Phishing) and extortion attempts were the two most common types of threats people received.
- And finally, the good news is that BGP-style Internet routing security, measured as the share of valid routes, improved globally during 2023. Significant improvement in routing security was observed in countries including Saudi Arabia, the United Arab Emirates, and Vietnam.

So, overall, no big surprises and overall, when viewed from 20,000 feet, the Internet remains largely stable. It's cool to see the emergence of some post-quantum crypto protocol usage and I'm still surprised that there could be year-over-year growth of 25% in overall traffic.

SpinRite

The announcement I expected two weeks ago to be able to make last week, was that I had finally accomplished the surprisingly challenging task of on-the-fly remote server-side EV code signing using a hardware security module. It's a capability I've wanted to have for years... and although it took far more time than I expected, since every aspect of the project fought back, that technology now exists. It's in place and appears to be working reliably. I brought it online last Saturday morning for cautious testing by the gang in GRC's development newsgroup, and more than 150 instances of SpinRite's current release candidate #5 were successfully built, on-the-fly signed, downloaded and tested.

I decided to obtain a fresh 3-year EV code signing certificate from DigiCert for the HSM, since the one I had was a year old and I wanted to get as long a run from the appearance of this new certificate as possible. As we know, reputation is now the way the world works. Not surprisingly, a few people reported that Windows Defender was upset, quarantined and deleted their download. But most people said that Defender didn't make a peep and that everything worked for them without a hitch. My hope is that by the time SpinRite 6.1 is being heavily downloaded, Microsoft will have had time to decide that all is well with it. I just grabbed a fresh copy and dropped it on VirusTotal. It triggered 0 out of 68 tests. No A/V engine had any problem with it. But during my testing I tried that with unsigned code and at least one third of them freaked out. So I conclude that this was time well spent.

Where I am today is that SpinRite is all but finished. I'm actually a bit happy that the code signing project took four weeks, because during that time many more people have had the chance to use the current release candidate. This has surfaced some remaining edge cases that I would like to resolve before I formally declare SpinRite 6.1 finished.

I could ship it now, but on really troubled drives it can still stumble a bit. And since "really troubled drives" is definitely one of SpinRite's targets, I want to at least know that there's nothing more that can be done. For example, there have been some reports of very troubled drives dropping offline when SpinRite touches a particularly sensitive spot on the drive. This is something we encountered many times during our early testing. SpinRite pops up a scary red dialog to explain that after being reset, the drive never reported that it was ready for more. SpinRite waits for up to ten seconds while checking the drive's status every 10 milliseconds before it makes that determination. If you watch the seconds tick by on a clock, 10 seconds is a long time. But over this past weekend I've verified that for really troubled drives it might not be long enough. In this instance, SpinRite needs to be even more patient. So starting with the next release, SpinRite will give drives a full 60 seconds to get themselves back up and ready to proceed. And since SpinRite's user may wonder what's going on while nothing appears to be happening, after waiting several seconds, SpinRite will display a "Waiting for drive: xx" count down so that its user knows why nothing appears to be happening.

Since we're so close to the end of 2023, and I'd like any recent improvements to have a bit of time for testing, I figure I'll fuss with it for the rest of the year and make it available at the start of 2024. I recognize that even after its official release, I may still be tempted to deal with even edgier edge cases. And any improvements I'm making at this point all feed forward into SpinRite 7's design anyway, so it's time well invested. I have the feeling that I may be continuing to nudge it along for a while. In this day and age, it's so easy for any SpinRite owner to obtain the

latest update that there's no reason for me not to improve what I can.

Closing the Loop

A listener Tweeted:

I'm not going to pretend to understand the details of this, but @SGgrc and other authorities have deemed this a major step forward in quantum computing. @bitcoincoreorg — what is the plan for post-quantum implementation? Current asym crypto is threatened.

This listener was clearly referring to last week's "Quantum Computing Breakthrough" topic. And he's correct that asymmetrical crypto using the algorithms in use today will not be in use in the future. The good news is that things like iterative PBKDF hashing of passwords to obtain a fixed-size token are not asymmetric so they will remain safe. I'm mentioning this, first because that's something important to appreciate. The world's password-accepting websites will not need to revamp their traditional password hashing systems. But also, and blessedly, neither will the operation of the Bitcoin Blockchain. Recall that the way Bitcoins are earned is by guessing what needs to be appended to the most recent blockchain update in order to yield a hash result that ends in some number of trailing 0's. While GPUs have proven to be quite facile at performing the hash function needed to guess at very high rates, choosing a random value and hashing the result is not something that is suited to tomorrow's quantum computers. And thank goodness for the fact that symmetric crypto will not be affected by quantum computing, because otherwise we would be in much more serious trouble than we are now.

Philip Griffiths / @ThePGriffiths

Hey Steve, 952 you mentioned ZeroTier and Tailscale as open source. "Sort of" is my opinion. ZeroTier is BSL, so open source to many, but not everyone. Tailscale is largely open source but core parts, eg. the coordination server are not.

Netbird or Headscale would be better examples of overlays which are OSS and allow circumvention of NAT. You could also include OpenZiti, though you could also argue, while it can be used as a better VPN, its true design goal is to make it easier to build secure-by-default, distributed applications.

Although much of Tailscale is open source, Tailscale have retained some pieces, those are the GUI clients for Windows, macOS and iOS, and the control server. So Headscale implements a self-hosted, fully open source alternative to the Tailscale control server. Headscale's goal is to provide self-hosters and hobbyists with an open-source server they can use for their projects and labs. It implements a narrow scope, a single Tailscale overlay network suitable for personal use, or a small open-source organization.

Netbird looks like another interesting fully open source overlay network using Wireguard for its transport security and encryption. OpenZiti isn't a general purpose overlay network. It's a system of technology, language APIs and SDKs that allow developers to incorporate secure overlay network technology into their apps. So it's a different solution than Tailscale, ZeroTier or Netbird.

As for how those three compare, I'm unable to offer any comparison or recommendation. I haven't yet had the need to deploy any of them so I haven't given them a very close look. When I do I'll definitely share a full review.

Comm Tech Engineer / @engineer_comm

A quick question on Spinrite. Do the hardware specs (better CPU or more RAM) of the PC running Spinrite effect the speed of Spinrite operations?

I've seen this question several times before, so I thought I'd answer it for everyone. The answer is almost always no – the hardware doesn't matter. SpinRite will detect and alert its user when a SATA III (6 gigabits per second drive) and is connected to a SATA II interface which is only able to run at 3 gigabits per second. Though even 3 gigabits per second is sufficient for any spinning drive. But as for CPU and RAM, SpinRite 6.1 does use about 50 megabytes of RAM, but it's rare to find a machine today with fewer than 4 gigabytes, and even one gigabyte would be fine. Not one of our more than 800 testers have ever encountered a machine with insufficient RAM for SpinRite 6.1. And the same is true for the CPU under v6.1. So it's almost always true that any old hand-me-down PC can be used as a dedicated SpinRite test machine, and many of SpinRite's owners do exactly that. Even though SpinRite 6.1 is much faster than 6.0, and is now able to keep any directly attached drive running as fast as it's capable of going, drives have become ridiculously huge and it does still take time to move all of that data back and forth. But it's the drive's ability to move data to and from its actual storage media that's now the bottleneck, never the system's CPU or RAM.

A listener who requested anonymity

I'm listening now to SN950, and I wanted to share my experience with trying Passkeys on GitHub. Before passkeys, I had username, password, and MFA. After enabling passkeys and using them as the authentication method, GitHub no longer prompts for another factor, so it seems the security of the MFA has disappeared. I store my MFA seeds outside my password manager. If, however, I were to store my passkeys within my password manager, I would then reduce my security for any site that skips MFA when using passkeys.

I understand that passkeys are better than passwords as the site no longer has a secret to protect, but all the necessary "eggs" would still be in my password manager's basket. I think passkey + MFA would provide the highest level of security, but I don't know which sites will allow/offer that option, and which will drop MFA while using passkey authentication under the assumption that multiple factors are now longer necessary, as GitHub appears to assume. For those with the strictest threat model, I think I would recommend NOT storing passkeys in the same password manager as everything else. Am I missing something here?

Also, I never use Twitter myself, and so I'd be one of those looking forward to your new email list. I had to dust off my login from years ago just to write this to you. :)

Like this listener, I'm a bit distressed to learn that the use of passkeys automatically disables the use of additional authentication factors – especially for a site such as GitHub where improving authentication integrity has been a recent issue. As we know, passkeys are stronger than usernames and passwords for a number of reasons. But this listener is correct about the

vulnerability inherent in allowing any single device to have full authority to authenticate us, no matter how strong its authentication mechanism might appear to be. The right solution would be to offer users who are adopting Passkeys the option to disable their additional authentication factors in favor of passkeys since passkeys are certainly stronger than passwords alone. Or to keep additional authentication factors in place and enabled under the more proper understanding that **any** single factor of authentication, regardless of how strong it may be by itself, can still be made more strong by the requirement for any additional factor – especially one that relies upon another device and uses an entirely different technology – such as time varying 6-digit tokens.

SKYNET / @fairlane32

Hi Steve, re: SN-952 and upstream library dependencies: What is this notion that developers have that fixing a bug will automatically introduce something new that will break? How is it not possible to fix a flaw without introducing a new feature that will break something else? It seems that everyone, including Microsoft, cannot fix a flaw or vulnerability without breaking something else. Why are they so connected, and how? How is it that a bug or flaw that needs to be fixed will just automatically break something totally different, totally unrelated to the bug? I know it is most certainly possible for companies to fix flaws without breaking something new in their products, so I find it a poor excuse for developers to claim that "it's all working right, so I don't want to rock the boat and possibly break something else." To me that just screams that either everything in their code is connected (bad) or they are shitty coders.

Last week's discussion more specifically related to a fear of updating upstream libraries, which are inherently black boxes, in a situation where the successful functioning of their own code is entirely dependent upon the exact behavior of those blocks boxes. The point being, everything is working now, let's not rock the boat. In highly complex projects mistakes do happen. Say that a group of people decide to entirely re-code some library because its codebase has grown so old and creaky over years of tweaking. That does happen, and re-coding can be a really good thing to do. But try as they might, it could be that this new code – which is intended to behave just the same as the original code – nevertheless exhibits some slightly different behavior around the edges and that this change, even if it's subtle, might cause some other code that uses the newly re-coded library to break. It's a mess, but it's a mess we've created and the motivations behind "don't fix it if it's not broken" is, I think, understandable.

Blaine Trimmell / @blainejt

I just listen to the security now podcast and want to pass on that Chromium browser does not use OS root store any more by default:
<https://blog.chromium.org/2022/09/announcing-launch-of-chrome-root-program.html>

Blaine's Twitter DM included a link to Google's announcement about three months ago on September 19th. Under the headline "Announcing the Launch of the Chrome Root Program", Google wrote:

In 2020, we announced we were in the early phases of establishing the Chrome Root Program and launching the Chrome Root Store. The Chrome Root Program ultimately determines which

website certificates are trusted by default in Chrome, and enables more consistent and reliable website certificate validation across platforms. This post shares an update on our progress and how these changes help us better protect Chrome's users.

Chrome uses digital certificates (often referred to as "certificates," "HTTPS certificates," or "server authentication certificates") to ensure the connections it makes on behalf of its users are secure and private. Certificates are responsible for binding a domain name to a public key, which Chrome uses to encrypt data sent to and from the corresponding website. As part of establishing a secure connection to a website, Chrome verifies that a recognized entity known as a "Certification Authority" (CA) issued its certificate. Certificates issued by a CA not recognized by Chrome or a user's local settings can cause users to see warnings and error pages.

Root stores, sometimes called "trust stores", tell operating systems and applications what certification authorities to trust. The Chrome Root Store contains the set of root CA certificates Chrome trusts by default. A root program is a governance structure that establishes the requirements and security review functions needed to manage the corresponding root store. Members of the Chrome Security Team are responsible for the Chrome Root Program. Our program policy, which establishes the minimum requirements for CAs to be included in the Chrome Root Store, is publicly available [here](#).

Historically, Chrome integrated with the root store and certificate verification process provided by the platform on which it was running. Standardizing the set of CAs trusted by Chrome across platforms through the transition to the Chrome Root Store, coupled with a consistent certificate verification experience through the use of the Chrome Certificate Verifier, will result in more consistent user and developer experiences.

Launching the Chrome Root Program also represents our ongoing commitment to participating in and improving the Web PKI ecosystem. Innovations like ACME have made it easier than ever for website owners to obtain HTTPS certificates. Technologies like Certificate Transparency promote increased accountability and transparency, further improving security for Chrome's users. These enhancements, only made possible through community collaboration, make the web a safer place. However, there's still more work to be done.

We want to work alongside CA owners to define and operationalize the next generation of the Web PKI. Our vision for the future includes modern, reliable, highly agile, purpose-driven PKIs that promote automation, simplicity, and security - and we formed the Chrome Root Program and corresponding policy to achieve these goals.

We talked about this three years ago, back in 2020 when Google announced this plan. But I had missed Google's announcement that this initiative was ready and was now being rolled out. So thank you, Blaine, for this update.

This of course means that both Google with Chrome, the various Chromium browsers, and Firefox, will all be running with their own local root stores. And given that, as we've seen, just six or seven CA root certificates are all that most users will ever need, that doesn't seem like such a big deal. But all of this is relevant, of course, because of the EU's Article 45. What is going to happen?

"Active Listening"

A story blew up in the news last week that currently lacks solid evidence, but it has certainly worried and upset everyone who has heard it. I suspect that this is the sort of thing that investigative reporters will be digging into further. The short version of the news is that the massive media giant CMG – the Cox Media Group – claims in its marketing materials to advertisers and in actual discussions with prospective clients, that it currently has and is using the capability, which their marketing materials term "Active Listening" to listen into the ambient conversations of consumers through microphones embedded in their smartphones, smart TVs, and other similar devices, and that through this means they are able to gather data which they then use to target advertising.

Last Thursday's headline in 404media, which broke the story, was: "Marketing Company Claims That It Actually Is Listening to Your Phone and Smart Speakers to Target Ads". They wrote:

The news signals that what a huge swath of the public has believed for years—that smartphones are listening to people in order to deliver ads—may finally be a reality in certain situations. Until now, there was no evidence that such a capability actually existed, but its myth permeated due to how sophisticated other ad tracking methods have become.

Exactly three weeks ago, on November 28th, the CMG website posted a blog page titled "Active Listening: An Overview." they also had a permanent page linked off their domain's root with the URL: "/cmg-active-listening". So, at the time it, was all right out there for the world to see. And this is not some fly-by-night sketchy operation; this is the Cox Media Group. To no one's surprise, all of those pages have since disappeared – though it's really worth noting that they were initially completely public and no one at Cox thought they, nor their "Active Listening", was a problem.

Fortunately, those pages were up long enough to have been crawled by the Internet's historian, the Web Archive and this week's shortcut of the week <https://grc.sc/953> will take your browser directly to a faithful copy of the archived blog posting made three weeks ago:

<https://web.archive.org/web/20231214235444/https://www.cmglocalsolutions.com/blog/active-listening-an-overview>

So what do we learn directly from this once-publicly posted page? It does not disappoint. The page shows a photo of four young hip consumers in their late 20's or early 30's gathered around a table, smiling and chatting with a Mac and a tablet. And the page says:

Imagine a world where you can read minds. One where you know the second someone in your area is concerned about mold in their closet, where you have access to a list of leads who are unhappy with their current contractor, or know who is struggling to pick the perfect fine dining restaurant to propose to their discerning future fiancé. This is a world where no pre-purchase murmurs go unanalyzed, and the whispers of consumers become a tool for you to target, retarget, and conquer your local market. It's **not** a far-off fantasy—it's **Active Listening** technology, and it enables you to unlock unmatched advertising efficiency today so you can

boast a bigger bottom line tomorrow. Do we need a bigger vehicle? I feel like my lawyer is screwing me. It's time for us to get serious about buying a house—No matter what they're saying, now you can know and act.

A marketing technique fit for the future. Available today.

Machine learning algorithms are improving and introducing a new era for advertising. Our Active Listening tech gives you a weekly roster of qualified customers who have voiced their need for your service or product. We then upload the list to your preferred advertising platforms so you can target ads to the right people at the right time. Reactive advertising is no longer enough to get ahead. Embracing predictive and proactive strategies is the key to growth.

Active Listening gives organizations clarity into the most effective channels and timing for their advertising efforts. **By incorporating and analyzing customer data gleaned from conversations happening around smart devices, we can pinpoint where and when customers are most likely to engage with ads.** When you have this information in reach, you have the power to deploy targeted campaigns at opportune moments on the platforms where your audience spends their time. The results? Maximized visibility and impact.

Whether you're a scrappy startup or a Fortune 500, Active Listening makes the unreachable in-reach.

How does it all work?: Advertise to the exact people who need your services. CMG can customize your campaign to listen for any keywords or targets relevant to your business. Here is how we do it:

Create personas: We flesh out comprehensive buyer personas by uploading past client data into the platform.

Identify keywords: We identify top-performing keywords relative to the type of customer you are looking for.

Transparent tracking: We set up tracking via pixels placed on your site so we can track your ROI in real-time.

Leverage AI: AI lets us know when and what to tune into. ***Our technology detects relevant conversations via smartphones, smart TVs, and other devices.***

Analyze consumer behaviors: As qualified consumers are detected, a 360 analysis via AI on past behaviors of each potential customer occurs.

Create a list: With the audience information gathered, an encrypted evergreen audience list is created.

Target, retarget, transcend: We use the list to target your advertising via many different platforms and tactics, including:

Streaming TV/OTT / Streaming Audio / Display Ads / Paid Social Media / YouTube and Google/Bing Search.

Don't leave money on the table-claim your territory now!

Our technology provides a process that makes it possible to know exactly when someone is in the market for your services in real time, giving you a significant advantage over your competitors. Territories are available in 10 or 20-mile radiuses, but customizations can be made for regional, state, and national coverage.

And then there's a link with the phrase: **Claim your territory now!**

Then they provide a handy FAQ where the first question they ask themselves is: "Is Active Listening Legal?" to which they reply:

We know what you're thinking. Is this even legal? The short answer is: yes. It is legal for phones and devices to listen to you. When a new app download or update prompts consumers with a multi-page terms of use agreement somewhere in the fine print, Active Listening is often included.

Uh huh... so why, exactly, has the CMG website been totally scrubbed of all mention of Active Listening? Perhaps strict legality is not the problem here. Next question:

Q: How Does Active Listening Technology work?

Our technology is on the cutting edge of voice data processing. We can identify buyers based on casual conversations in real time. It may seem like black magic, but it's not - it's AI. The growing ability to access microphone data on devices like smartphones and tablets enables our technology partner to aggregate and analyze voice data during pre-purchase conversations.

The result? Advertising efficiency and timing taken to a new level. We set specific keywords relevant to your product and service so we know who needs you, why they do, and where we can target them. With this unprecedented understanding of consumer behavior, we can deliver personalized ads that make your target audience think: wow, they must be a mind reader.

(Right! ... and that's not creepy at all!)

404 Media also found a representative of the company on LinkedIn who was explicitly asking interested parties to contact them about the product. One marketing professional pitched by CMG on the tech said a CMG representative explained the prices of the service to them. So it certainly appears to have been available. CMG's website says: "What would it mean for your business if you could target potential clients who are actively discussing their need for your services in their day-to-day conversations? No, it's not a Black Mirror episode—it's Voice Data, and CMG has the capabilities to use it to your business advantage."


The part of CMG advertising the capability is CMG Local Solutions. CMG itself is owned by Apollo Global Management (a hedge fund) and Cox Enterprises, which includes everyone's favorite residential cable provider and ISP Cox Communications. CMG operates a wide array of local news television and radio stations.

With Active Listening, CMG claims to be able to *"target your advertising to the EXACT people you are looking for,"* with the goal to target potential clients or customers based on what they say in *"their day to day conversations."* Then they provide some examples:

Imagine This...

What could it do for your business, if you were able to target potential clients or customers who are using terms like this in their day to day conversations:

- ✓ The car lease ends in a month- we need a plan.
- ✓ A mini van would be perfect for us.
- ✓ Do I see mold on the ceiling?
- ✓ We need to get serious about planning for retirement.
- ✓ This AC is on it's last leg!
- ✓ We need a better mortgage rate.



- The car lease ends in a month—we need a plan.
- A mini van would be perfect for us.
- Do I see mold on the ceiling?
- We need to get serious about planning for retirement.
- This AC is on its last leg!
- We need a better mortgage r

So, according to CMG's now-removed web pages, the way this works is that clients can "claim" a territory where they want to use CMG's services, which are available in a 10 or 20 mile radius. After setup, *"Active Listening begins and is analyzed via AI to detect pertinent conversations via smartphones, smart tvs and other devices,"* the website adds. CMG also claims it installs a tracking pixel on its client's website to monitor the return on investment (ROI). With an audience created, CMG then delivers advertisements to these people through streaming TV, streaming audio, display ads, YouTube, Google and Bing search.

The marketing professional who was pitched by CMG told 404 Media that after a call with the company, they disabled microphone access on much of their own technology: *"I immediately removed all my Amazon Echo devices and locked down microphone permissions on things like my phone. Receiving confirmation that they are doing things like this have confirmed my worst*

fears and I, for one, will take no part in it."

For its part, while CMG was busily removing all traces of this from their website, they told 404 media:

"CMG Local Solutions markets a wide range of advertising tools. Like other advertising companies, some of those tools include third-party vendor products powered by data sets sourced from users by various social media and other applications then packaged and resold to data servicers. Advertising data based on voice and other data is collected by these platforms and devices under the terms and conditions provided by those apps and accepted by their users, and can then be sold to third-party companies and converted into anonymized information for advertisers. This anonymized data then is resold by numerous advertising companies. CMG businesses do not listen to any conversations or have access to anything beyond a third-party aggregated, anonymized and fully encrypted data set that can be used for ad placement. We regret any confusion and we are committed to ensuring our marketing is clear and transparent."

Now here's something to think about...

Why is Cox doing this? They would not seem to be an obvious entity to create such a service. If, as they claim, all of the data is being aggregated by 3rd parties and they are just the middleman who is not directly doing any data gathering themselves, then there's nothing Cox is bringing to the table. Any random organization could do this. But they certainly do appear to have been all gung ho into it. If I were a betting man, I'd put my money on this being an adjunct to all of the massive amount of data that Cox Communications – the Internet ISP – **is already obtaining** from monitoring all of their Internet consumers' available Internet traffic; meaning all DNS query and TLS handshake metadata.

Cox, like any ISP, is sitting on a treasure trove of extremely valuable personal data: everywhere everyone in our family goes on the Internet. And Cox consumers are not anonymous to Cox. Cox knows exactly who and where every household is – they pay their bill every month. And now we know something we didn't directly know before: Now we know who Cox is and what they're really thinking. They're quite willing to hide in the fine print of, in their own words *"multi- page terms of use agreements"*.

I'd be much less worried about microphones – which at least for our very secure smartphones seems like a red herring – than about the fact that an organization such as Cox has just shown itself to be, is the conduit through which all of its subscribers' residential Internet traffic flows. I think the time has come to think seriously about bringing up encrypted DNS for residential Internet users. We do not know for sure whether "Active Listening" applies to audio. But given what we have just seen, it seems very unlikely that Cox and its ISP ilk are leaving any money on the table by **not** "Actively Listening" to everything they're able to obtain by monitoring all of their subscribers' use of the Internet, through our PCs, our smartphones and any other user-directed Internet devices. Given the evidence it seems clear that if they get it, and sell it, they will.

As a result of what was found on Cox's website, the threat of that sort of monitoring being done by a major residential ISP became far less theoretical and far more likely.

At this point I'm sure many of our listeners are thinking "*That seems like a good idea. How do we go about making that happen?*" – which I think that'll be a great topic for us to look at closely in 2024, which is only a few weeks away.

And speaking of which, I want to personally wish, and I know Leo and all of the TWiT network joins me, in wishing all of our listeners a happy and safe holiday season. 2024 promises to be at least as interesting as recent years, and we'll be right here to watch and examine as all of its events unfold.

See you then!!

