Episode Book

EPISODE #6560

Chrome, Firefox, and Verifiable Privacy Claims

PUBLISHED	13 November 2026 at 20:26 UTC
DURATION	29:31
LISTEN	myweirdprompts.com/episode/chrome-firefox-verifiable-privacy-63195/
HOSTS	Corn, Herman, Hilbert
SCRIPT MODEL	z-ai/glm-5.3
VOICES	chatterbox-regular (chatterbox-local)
PIPELINE	V5.26
SOURCES	25 cited by the research (listed at the end)
BOOK GENERATED	14 November 2026 at 06:47 UTC

SYNOPSIS

Trusting a tech giant like Google over a smaller privacy vendor comes down to a bet on incentives, but verifiability matters more than company size. This breakdown compares what Chrome collects by default, why Google's Privacy Sandbox failed, and how Firefox's built-in tracker blocking actually works. It also examines Proton VPN's independent Securitum audits and why skepticism of Romanian VPNs like CyberGhost rests on outdated law.

TRANSCRIPT



Corn

A friend comes over, glances at your screen, and reacts like you've been keeping expired dairy in the fridge. That's how this one starts. Daniel writes that a friend of his, pseudonym Marcus, visited recently and was horrified to learn he's used Chrome as his main browser for years. Marcus runs Proton for everything. Daniel's counter-position is that he trusts Google, a big company with a lot to lose, more than a small startup, and he puts people who fear government spying but trust a random Romanian VPN in the same bucket of the wrongly worried. What Daniel actually loses sleep over is tracking pixels and the way any contact with an organisation gets treated as consent to a drip-marketing list. He wants both positions steelmanned, and an actual verdict on whose priorities are backwards.



Herman

And he's asking us to be fair about it, which is harder than it sounds, because both of these men are confident and both of them are partially aiming at the right thing.



Corn

So let's do the steelman first. What does Marcus actually have a point about?



Herman

More than Daniel probably wants to hear. But before we get into it, I think the real question here isn't is Chrome bad. It's what is the actual threat model for an ordinary person, and does either of them have it right? Because Marcus and Daniel aren't really disagreeing about facts. They're making two different bets about what goes wrong.



Corn

Marcus bets that systemic, invisible data collection is the bigger risk. Daniel bets that the specific, visible intrusions are the ones that matter.



Herman

Marcus's posture is structural distrust of ad-funded surveillance. He prefers audited third-party tools, smaller players whose entire business is the privacy promise. Daniel's posture is institutional trust plus scepticism of security theatre from small vendors. Neither posture is stupid. Both are bets about where the damage actually lands, and the



Herman (continued)

interesting part of this episode is testing both bets against what's actually documented.



Corn

There's a twist coming, isn't there.



Herman

There is. The thing neither of them is worried about turns out to be, on the documented harm, probably the thing that matters most for an ordinary person. But I don't want to spoil it, because we get there honestly. We did an episode ages ago on the gap between messaging apps' privacy claims and what they actually collect, and the theme back then was the same: the promise and the plumbing are different animals. Today's version of that is verifiability. Which claims can someone outside the company check?



Corn

So, Marcus's case. Concretely, what lands on Google's servers when I open Chrome and just... browse.



Herman

Start with what's on by default, because this is the part people get wrong in both directions. Usage statistics and crash reports are sent by default. And the crash reports, from Google's own help page, may include site URLs, your activity before the crash, and the contents of the memory at the time of the crash.



Corn

The contents of memory at the time of the crash. That's a sentence that sounds technical until you realise memory contains whatever page you were on, whatever you'd typed.



Herman

Right. A crash report is a photograph of a moment, and the moment it photographs is you doing something. Chrome attaches a random identifier to these reports, and the identifier resets every time you toggle the setting, which sounds reassuring, except the toggling itself is the boundary. If you're signed in, the usage statistics may include the age and gender on your Google Account, so the anonymisation has a leak built into it the size of a login.



Corn

A random number that knows your birthday.



Herman

Now, the misconception to kill here: Chrome does not send your full browsing history to Google by default. There's a separate opt-in called Make searches and browsing better, which sends URLs of pages you visit. And Google's own description says that once received, URLs known to Google are stored and unknown URLs are discarded.



Corn

Which is almost worse. It's not I'm not collecting, it's I'm only keeping the interesting ones.



Herman

The bigger surface, honestly, is Sync. Bookmarks, history, open tabs, passwords, payment info, settings, all sitting in your Google Account. That's the single largest collection of data most Chrome users have ever handed anyone, and they did it voluntarily, because Sync is convenient and mostly invisible. Then the advertising layer: Google's ad server logs include your IP address, browser type, one or more cookies that may uniquely identify your browser, or, if you're signed in, may uniquely identify you. They anonymise part of the IP after nine months and cookie information after eighteen.



Corn

Eighteen months. That's a business quarter times six, if the internet's counting.



Herman

And Google says plainly that it may infer whether activity from different devices, browsing sessions, or accounts is associated. Cross-device linkage by inference. Turning off personalised ads is not a clean exit either. Even with cookies removed, Google may use cookie-based information or other ad technologies unless you change the ads settings, and even then you still see ads based on IP-derived location, browser type, and search terms. So the off-ramp has an off-ramp, and that one has a toll.



Corn

The steelman reads: a default-on telemetry stream coupled to the world's largest advertising business. What does Marcus's friend Marcus... what does Marcus say to that?



Herman

He'd point at the Privacy Sandbox, and honestly this is the strongest evidence on his side of the ledger. Google spent years building a privacy-preserving ad system. Topics, Attribution Reporting, Protected Audience. The idea was to keep advertising working without third-party cookies following you around. Adoption never came. The Topics API went from about thirteen percent of page loads when Google announced the deprecation intent in November twenty twenty-five, down to under five percent by June, down to about two percent by September of this year. Google killed it. Anthony Chavez, the VP for Privacy Sandbox, announced the retirement in October last year citing, roughly, deepened understanding of what drives value. Which is corporate for nobody used it.



Corn

And then the interesting bit.



Herman

When Chrome one fifty shipped in July, the user-facing Ad Privacy settings page, the toggles for ad topics, site-suggested ads, ad measurement, vanished. No announcement, no release note. The address that used to take you there now just redirects to the main settings page. Google's own documentation hadn't caught up with it.



Corn

So the privacy engineering died of market indifference, and the privacy controls were quietly deleted. That's the part I'd want Marcus to say out loud, because it's the one thing in this whole story that's a pattern rather than a setting.



Herman

The counter-read, to be fair, is that the tracking Privacy Sandbox was meant to replace never went away. Chrome kept third-party cookies. So it's not that Chrome tracks you more than before, it's that the attempt to track you less was abandoned and the controls were tidied up after the funeral.



Corn

What's Marcus's browser, then, actually getting him? Firefox. Give me the honest comparison, because the folklore version is Firefox equals clean.



Herman

The folklore is wrong in a useful direction. Firefox ships Enhanced Tracking Protection on by default, blocking third-party tracking cookies, since Firefox sixty-nine in twenty nineteen. Total Cookie Protection, which partitions all third-party storage into per-site jars, became default in twenty twenty-two. Mozilla published new fingerprinting research just three days ago, on making Firefox users harder to fingerprint, reducing the distinguishing details so tracking scripts see more users as the same person.



Corn

And Chrome's default tracker blocking is...



Herman

Not there. Chrome has no built-in tracker blocking by default. That's a real structural difference. But Firefox is not telemetry-free, and I refuse to let Marcus believe it is. Mozilla collects technical and settings data. Firefox runs ads on the New Tab page, and collects interaction data on that sponsored content, shared with advertising partners on an aggregated or de-identified basis. Your search queries go to your search provider as you type, as suggestions, though in the US Mozilla routes its own suggestions through an encrypted proxy setup to hide your IP.



Corn

So the difference is the deal, not the amount. Chrome's telemetry feeds the same company that buys the ads. Firefox's telemetry feeds a foundation whose revenue comes from search deals.



Herman

That's the honest one-liner. Structurally different incentives, not zero collection. Anyone who tells you their browser collects nothing is selling something, and in Mozilla's case what they're selling is ads on the New Tab. I find that grimly funny, given Mozilla's name. Corn has a whole bit about that.



Corn

A portmanteau of Mosaic and Godzilla, from a privacy nonprofit. I've made peace with it.



Herman

Now Daniel's side of the steelman, because it's stronger than the privacy community gives it credit for. There is no evidence Google sells Chrome browsing data to third parties in the ordinary sense. The framing everywhere in Google's own documents is ad personalisation within its own systems plus aggregate reporting. Do-not-sell searches turn up browser extensions' policies, not Google's.



Corn

That matters legally. A company that doesn't sell the data is a different animal from one that does, whatever the vibes say.



Herman

And Daniel's instinct about big-company risk is not crazy. Google's loss from a privacy failure is a fine and a headline. Chrome has about three point six billion users, roughly sixty-nine percent of the browser market. That's a lot of headline. The question is whether that asymmetry cuts toward trust or against it, and here's where I think Daniel's argument runs into a wall.



Corn

Go on.



Herman

His gain from ad targeting is not a side effect. It's the core revenue. His loss from a privacy failure is a fine he's already budgeted for. If you weigh what a company has to lose against what it has to gain, Google has a lot to lose and vastly more to gain, and the gain is recurring while the loss is one-time. That's before the antitrust dimension, where Google just escaped an ordered sale of its ad exchange in September and got behavioural remedies instead, so even the accountability mechanism is being negotiated down to conduct promises.



Corn

And Marcus's version of the same trust question is checkable. That's the part that swung me reading this.



Herman

Proton VPN's no-logs claim is independently audited. Securitum did their fourth consecutive annual audit on-site at Proton's Zurich headquarters over three days in August last year, and found no user activity logging, no metadata storage, no traffic inspection, including for free-tier users. There's since been a fifth audit published. Google's retention schedule is self-reported. One claim can be checked by a third party. The other cannot. Daniel's trust argument says trust the bigger company because it has more to lose. But the audited small player's entire business is the promise, and the promise is inspected annually by people who don't work there.



Corn

Verifiability beats size. I'd put that on the bumper sticker, but I move slowly and the traffic here is fast.



Herman

And that gets us to the Romanian VPN, because Daniel lumps fear-of-government types who trust a Romanian VPN into the worried-about-the-wrong-things bucket. And the jurisdiction part of that is simply out of date. Romania struck down its data retention laws in two thousand nine, and the Constitutional Court killed them again in twenty fourteen.



Herman (continued)

There's no retention duty reaching VPNs. CyberGhost is Bucharest-based and publishes quarterly transparency reports. Last quarter they logged over twenty-seven thousand DMCA complaints in July alone, thirty thousand in August, twenty-nine thousand in September, plus four police requests, and their position is that they run RAM-only infrastructure that resets, so the IP-to-person connection cannot be made on their network, and they cannot comply even with legally binding requests.



Corn

Four police requests against eighty-seven thousand complaints. Hollywood is really working that one domain.



Herman

So Daniel's heuristic, jurisdiction equals risk, is directionally reasonable but imprecise. The failure mode he fears is real in kind. There was a PureVPN incident involving a third-party vendor's server in Romania where specific data was exposed, even though the core no-logs data wasn't. The lesson there isn't Romania bad. It's that a no-logs promise is only as good as the infrastructure around it, which is exactly why audits matter. Marcus isn't trusting a random Romanian VPN, or at least he shouldn't be. He's trusting a Swiss one with an annual third-party inspection. Those are different sentences.



Corn

So on the browser question, where do I land? Marcus is directionally right and overstated. Chrome is not reckless, but the default posture serves the ad business, the off-ramps have off-ramps, and the one time Google built something privacy-preserving, the market ignored it and Google deleted the controls without telling anyone. That's not a browser review, that's a character reference.



Herman

I'd add one thing from the medical side of my brain, which is that the harm here is diffuse. Nobody gets stalked because Chrome usage statistics were on by default. The browser-layer harm is statistical: slightly better ads, slightly more inference, a slightly more complete model of you. Daniel's actual worries are the opposite shape, and that's where we should go next, because they're better-founded than he seems to think.



Corn

The pixel thing first. Because I remember his phrasing, disturbing, and I want to know if the reality earns it.



Herman

The reality is a one-by-one invisible image embedded in an email. When you open the message, your client loads that image from a remote server, and the load is the signal. The sender learns the open happened, from the IP address, which gives location. A unique URL is created per recipient, so it's individually attributable, and it logs every open, every forward-triggered open, and if you click a link, the click. The Canadian Centre for Cyber Security put out guidance last year saying pixels can track the location and behaviour of the recipient, and that this can be used for later attacks. Their mitigation is to configure your inbox not to load external images.



Corn

A national cyber agency describing marketing emails as an attack vector. That's Daniel's intuition with a government letterhead on it.



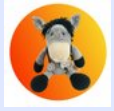
Herman

If you look at an actual tracking event payload, it's an email identifier, a subscriber identifier, a timestamp, a geolocation block with country. Modest, per-message, and utterly invisible to anyone who isn't looking for it. People who've dissected these describe exactly that: read receipts with an IP address attached.



Corn

Which is where I'd deflate Daniel a little. A read receipt with an IP address is surveillance, but it's bounded surveillance. It's not a profile of your life, it's a log of your mornings.



Herman

Agreed. The harm is real, per-message, individually attributable, and small. In the EU it's regulated too. The French regulator's guidance says measuring individual open rates or profiling requires consent; anonymous aggregate statistics are different. So Daniel's instinct is well-founded, and the harm is bounded. Both of those are true.



Corn

The drip-marketing one is the seam I want to pull at. Any contact gets treated as consent.



Herman

The seam exists, and it has a name in the law. Under GDPR, email marketing can rest on consent or legitimate interest. But the ePrivacy Directive sits on top and says marketing emails need consent, period, pending a regulation that's been pending for a decade. In practice, providers split the basis in exactly the way Daniel describes. I've seen privacy policies that assign responding to contact form inquiries to legitimate interest, and email marketing and drip sequences to consent, in the same document. The contact form is the hook, the drip sequence is supposed to need consent, and the gap between those two rows of the table is where the behaviour he hates lives.



Corn

So the form is the handshake and the drip list is the twelve-year subscription you agreed to by shaking.



Herman

The rules are stricter than people think. Consent has to be freely given, specific, informed, unambiguous. Legitimate interest suits retention updates, but it needs documented purpose, necessity, balancing tests. First-time outreach and behavioural profiling are supposed to need explicit consent. There's a right to object, and complaints can trigger automatic unsubscribe.



Corn

Let's hear what our listeners make of all this. We've got a voicemail from Mei.
Mei: Hi Corn and Herman, this is Mei, calling from the back of the two hundred and eleven bus heading home to Bedok, so if you hear an uncle snoring that is not me. I wanted to say I really enjoyed today's episode about Marcus and Daniel and whether using Chrome is reckless or whether they are both worried about the wrong thing, and I have a question that has been sitting with me since the bus left the interchange. My mother still uses Internet Explorer on the old desktop at home, and every time I visit she asks me to help her with the pop-ups, so I suppose my real question is whether the harm from a browser is about what it collects or about what it lets other people collect from you, because I feel like for her it is the second one, but I am not sure if that is a different topic entirely.



Corn

Internet Explorer in the wild. There's a museum exhibit walking around.



Herman

It's not a different topic, Mei's nailed something. Her mother's browser isn't collecting anything, nobody at Microsoft cares what she does in it. But an unmaintained browser lets other people's code run wild in it. The pop-ups she's fighting are exactly the what-it-lets-in category. The old browser is a door with a broken latch.



Corn

And that's the split worth naming for Daniel too, because it's the same fork. What the browser collects is Google's half of the deal. What it lets through is everybody else's half, and Chrome's default with no tracker blocking is weakest on the second half, which is the half that actually touches Mei's mum. Block external images in her inbox while you're there, by the way. Kills the pixels too.



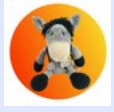
Herman

Two birds. Now the jurisdiction point, because it reframes Daniel's complaint completely. He's in Jerusalem. Under the EU and UK rules, drip marketing after a contact form is a compliance failure, not a legal vacuum. The seam is regulated and someone is abusing it. But most of the drip lists that follow Daniel around the internet were probably born in the US, where there's no equivalent rule at all. So the experience he's having isn't a broken system. It's the system working where it exists and not existing where it doesn't.



Corn

Which turns his complaint from the rules are fake into the rules are local. Less satisfying to be angry about.



Herman

Now, here's where the episode turns, and I want you to brace. Because the harms neither Daniel nor Marcus is worried about are the ones with the best-documented impact on ordinary people, and they're boring. People-search sites. Data brokers. The aggregation layer.



Corn

This is the part where you get going, so I'll just hold on.



Herman

Consumer Reports ran a study. Thirty-two volunteers, thirteen people-search sites, seven paid removal services, four months. The paid services removed thirty-five percent of the profiles. Thirty-five. Manual opt-outs, doing it yourself with a spreadsheet and a lot of patience, reached about seventy percent. The paid option did half the job of a stubborn person with free time. And Consumer Reports' framing isn't gentle: these sites put ordinary people at risk of fraud, identity theft, scams, stalking, harassment. This is where the harm stops being statistical. A stalker doesn't need Chrome's telemetry, he needs a nine-dollar directory listing with your home address on it.



Corn

And the services people pay to fix it. The academic numbers?



Herman

A twenty twenty-five study of four commercial removal services, including DeleteMe and Incogni, found under half of identified records were successfully removed. The best service managed about seventy-seven percent, the worst about twenty-three. And here's the detail that gets me every time: only forty-one percent of the records they identified were actually the participant's own information. The majority of what these services found and fought to remove belonged to someone else with a similar name. Meanwhile one independent review of a budget service found eighty percent removals. The variance between services is enormous. It's a market where you can pay a lot and get a coin flip, or pay a little and get most of it done, and there's no way to know in advance which is which.



Corn

You're being watched by four companies, defended by one, and the defender thinks you're someone else.



Herman

There's one more wrinkle from the compliance research on the California privacy law. When people submitted deletion requests, some brokers responded by requesting personal information as part of their identity verification process, including details they



Herman (continued)

had not previously collected. Your request to be deleted is a form that teaches them more about you.



Corn

The exit interview collects your data on the way out. Beautiful. In the sense that I want to burn something.



Herman

Here's my synthesis, and then I want your verdict, because you've been suspiciously quiet on the adjudication.



Corn

I've been adjudicating. Slowly. It's my method.



Herman

My read: neither of them is backwards, they're both misaimed. Daniel worries about pixels and drip marketing, which are real, regulated where he lives, and annoying. Marcus worries about browser-level profiling, which is real, systemic, and diffuse. Neither of them is worried about the aggregation layer, where the documented ordinary-person harm actually lives, and where the paid fix fails more than half the time. Daniel's trust in Google is structurally backwards, verifiability beats size. But his specific worries are more legitimate than he gives himself credit for, and Marcus's structural critique is right while his chosen battleground, the browser, is the wrong hill. The ordinary person should be spending their worry budget on people-search sites and on whether a privacy claim can be checked by someone who doesn't work at the company making it.



Corn

Then I'll give the verdict as a question back at Daniel. He put the Romanian VPN people and the government-fear people in a bucket called worried about the wrong things. Fine. But he's in a bucket too, and it's the one where you worry intensely about the harms you can see in your inbox and never once type your own name into a people-search site to check what a stranger sees. I'd bet the farm he's never done that. Marcus, either.



Herman

Neither have most people. That's the whole problem. The browser fight is legible. You pick Firefox, you feel different. Data broker aggregation is weather. You can't unsubscribe from weather.



Hilbert

CyberGhost had four police requests, not four. Four in September. Five across the quarter. I read the report at the weekend.



Herman

Five across the quarter. Fair enough, I collapsed the months.



Hilbert

The rest of it was right, which for this show is a good week. I'll tell you the part you left out. I spent three weeks this summer getting myself off a people-search site. Not for privacy reasons. The site listed me at a house I haven't lived in since the nineties, and the junk mail addressed to me kept arriving there, and the current occupants kept forwarding it to me with notes. The notes got shorter each time. So I went at the record. Four different brokers had copied it off each other, and correcting one did nothing to the other three, because they don't read each other's corrections. They read each other's mistakes.



Corn

The ingest pipeline is faster than the correction pipeline.



Hilbert

The removal process is filling out a form to tell a robot that you are who you say you are, so it can tell another robot, which will ignore it. I kept a spreadsheet. Date submitted, response received, record actually removed. And a fourth column I called lies, for when a broker wrote back confirming removal and the record was still there a week later. The lies column is the only one that filled up. Corn would have liked the spreadsheet. He takes three weeks to do things too.



Corn

I savour.



Hilbert

In the end I gave up on the brokers and wrote to the occupants of the old house instead, asking them to mark the mail return to sender, not at this address. Worked better than the removal services. Two shillings of postage did what four companies couldn't. I was in records management for a haulage firm for a while, and the rule there was that a record nobody maintains is a record nobody corrects. Same here.



Corn

Return to sender as a data subject request. There's a man at the mixing desk who beat an industry with a stamp.



Herman

The forwarding detail is the part I'd hang the whole segment on, honestly. He re-routed the physical mail instead of fixing the database, and the physical fix worked. It's the exact inverse of every privacy product on the market, all of which fight the database and none of which touch the letterbox.



Corn

If the browser isn't where the harm is, why does the privacy conversation keep returning to it? I think it's the visibility thing. The browser is a decision you can hold in your hand. Monday you use Chrome, Tuesday you use Firefox, you feel the difference. Nobody feels a broker aggregating a utility record.



Herman

Browser choice feels like identity, which is why Marcus was horrified and not merely concerned. Choosing Firefox is a statement about yourself in a way that opting out of a data broker never will be. The open question I'd leave with the audience is where this goes next. The Privacy Sandbox is dead, Chrome kept third-party cookies, and the controls vanished without an announcement. If that's the trajectory, the fight worth having isn't which browser, it's whether verifiability becomes the standard for privacy promises, audited claims, third-party checks, or whether size and reputation keep substituting for proof. Because the moment we all agree reputation counts as evidence, every company on



Herman (continued)

earth becomes trustworthy by press release.



Corn

On the reputation Daniel and Marcus both enjoy, our producer Hilbert Flumingtop keeps this desk running and this audio listenable. For more along these lines, there's episode thirty-five, The Privacy Gap; episode sixteen, On Deepfakes, SynthID, And AI Watermarking; and episode fifty-seven, From Lawyers in Limousines to Developers in Their PJs. This has been My Weird Prompts. If you've got a minute, the show is on Spotify, and a rating there helps more listeners find us.



Herman

You can find everything else at my weird prompts dot com. See you tomorrow, brother.



Corn

Tomorrow. If the brokers haven't found me by then.

SOURCES

What the research for this episode read before the script was written. Primary sources first.

1. **Google Chrome Help [primary]**
   How Chrome keeps your usage statistics and crash reports private, retrieved 2026-11-13
   https://support.google.com/chrome/answer/14746339?hl=en

2. **Google [primary]**
   Advertising (how Google uses cookies), retrieved 2026-11-13
   https://policies.google.com/technologies/ads?hl=en

3. **Google Chrome Enterprise Help [primary]**
   Chrome Sync and your data, retrieved 2026-11-13
   https://support.google.com/chrome/a/answer/13616205?hl=en

4. **Google Privacy Sandbox [primary]**
   Update on Plans for Privacy Sandbox Technologies, Anthony Chavez, 2025-10-17, retrieved 2026-11-13
   https://privacysandbox.google.com/blog/update-on-plans-for-privacy-sandbox-technologies

5. **Google Privacy Sandbox [primary]**
   Privacy Sandbox feature status, last updated 2026-08-14, retrieved 2026-11-13
   https://privacysandbox.google.com/overview/status

6. **Chromium blink-dev [primary]**
   Intent to Deprecate and Remove: Topics API, 2025-11-07, retrieved 2026-11-13
   https://groups.google.com/a/chromium.org/g/blink-dev/c/_R85yctz4Rs

7. **Mozilla [primary]**
   Firefox Privacy Notice, retrieved 2026-11-13
   https://www.mozilla.org/en-US/privacy/firefox/

8. **Mozilla Security Blog [primary]**
   Open research, stronger privacy: Making Firefox users harder to fingerprint, 2026-11-10, retrieved 2026-11-13
   https://blog.mozilla.org/security/2026/11/10/open-research-stronger-privacy-making-firefox-users-harder-to-fingerprint/

9. **Firefox Source Docs [primary]**
   Data Collection, retrieved 2026-11-13
   https://firefox-source-docs.mozilla.org/contributing/data-collection.html

10. **Proton VPN [primary]**
    Does Proton VPN keep logs?, retrieved 2026-11-13
    https://protonvpn.com/support/no-logs-vpn

11. **Proton VPN [primary]**
    Proton VPN passes 5th annual external audit of no-logs policy, retrieved 2026-11-13
    https://protonvpn.com/blog/no-logs-audit

12. **CyberGhost VPN [primary]**
    Quarterly Transparency Report Q3 2025, retrieved 2026-11-13
    https://www.cyberghostvpn.com/privacyhub/transparency-report-q3-2025/

13. **Canadian Centre for Cyber Security [primary]**
    ITSAP.60.002, Cyber security best practices for managing email, August 2025, retrieved 2026-11-13
    https://www.cyber.gc.ca/en/guidance/cyber-security-best-practices-managing-email-itsap60002

14. **U.S. DOJ [primary]**
    Department of Justice Wins Significant Remedies Against Google, retrieved 2026-11-13
    https://www.justice.gov/opa/pr/department-justice-wins-significant-remedies-against-google

15. **Google**
    Chrome Privacy Notice, archived 2021-09-23 (marked retired), retrieved 2026-11-13 [primary, archived]
    https://www.google.com/chrome/privacy/archive/20210923/

16. **PiunikaWeb**
    The last piece of Google's Privacy Sandbox is gone from Chrome, 2026-07-05, retrieved 2026-11-13
    https://piunikaweb.com/2026/07/05/chrome-150-removes-ad-privacy-settings/

17. **arXiv**
    The Rise and Fall of Google's Privacy Sandbox, retrieved 2026-11-13
    https://arxiv.org/html/2607.00693v1

18. **Measure The Web**
    Browser Protection reference table, retrieved 2026-11-13
    https://www.measuretheweb.org/privacy/browser_protection

19. **Tom's Guide**
    Proton VPN passes its fourth consecutive no-logs audit, 2025-09-24, retrieved 2026-11-13
    https://www.tomsguide.com/computing/vpns/proton-vpn-passes-its-fourth-consecutive-no-logs-audit-heres-what-that-means-for-your-data

20. **Le VPN**
VPN Logging Policies and Jurisdictions: 2026 Reference Table, retrieved 2026-11-13
https://www.le-vpn.com/no-log-vpns-privacy-jurisdictions/

21. **Acciyo**
Understanding the PureVPN Romania Leak (updated Nov 2026), retrieved 2026-11-13
https://www.acciyo.com/understanding-the-purevpn-romania-leak-what-you-need-to-know-in-2025/

22. **Tuta**
What is a tracking pixel?, retrieved 2026-11-13
https://tuta.com/blog/what-is-pixel-tracking

23. **Privacy Cats**
Guide: Tracking Pixels in Email (based on CNIL guidance), retrieved 2026-11-13
https://privacycats.com/posts/guide-tracking-pixels-in-email/

24. **Beng Tan**
What's in email tracking links and pixels?, retrieved 2026-11-13
https://bengtan.com/blog/whats-in-email-tracking-links-and-pixels/

25. **GDPR-Info**
Email Marketing, retrieved 2026-11-13
https://gdpr-info.eu/issues/email-marketing/