CITP

CITP.PRINCETON.EDU

INSTITUTE FOR TECHNOLOGY LAW & POLICY
GEORGETOWN LAW

Digital Fingerprinting: A Technical Briefing

FEBRUARY 2026

Introduction

Third-party cookies are on their last legs. Safari has blocked them by default since 2020, and Firefox's Enhanced Tracking Protection has followed suit.[1] Apple's App Tracking Transparency, launched in 2021, requires apps to obtain explicit permission before tracking; most users say no.[2] For a while, it appeared that Google would eventually drop support for third-party cookies in Chrome, but the company has since reversed course, opting instead for a "user choice" model that maintains the cookie while rolling out "IP Protection" to mask certain signals.[3] State privacy laws now mandate honoring opt-out signals, and the tracking infrastructure that powered digital advertising for two decades is fragmenting.

Even with the potential deprecation of third-party cookies, other methods will emerge that achieve the same monetization objectives through cross-site user identification, behavioral profiling, targeted advertising, and dynamic pricing. The industry response has been to move tracking somewhere users cannot see or control. This is where techniques such as device fingerprinting can be observed.

Device fingerprinting assembles a unique identifier from a device's observable characteristics: screen resolution, installed fonts, graphics card rendering, audio processing quirks, timezone, language settings, and dozens of other signals. Unlike cookies, this identifier requires no local storage. The device reveals it simply by functioning normally. Users cannot clear it because there is nothing stored to clear. Browser settings designed around cookie management do not help. The fingerprint regenerates instantly from unchanged device characteristics.

---

[1] WebKit, "Full Third-Party Cookie Blocking and More" (March 2020), https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/; Mozilla, "Enhanced Tracking Protection in Firefox," https://support.mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop.

[2] Apple, "App Tracking Transparency," https://developer.apple.com/documentation/apptrackingtransparency

[3] Google, "A new path for Privacy Sandbox on the web" (July 2024), https://privacysandbox.com/news/privacy-sandbox-update/

This is not a new technique. Researchers have documented fingerprinting since at least 2010[4]. What is new is its context. As cookie-based tracking becomes less viable, fingerprinting becomes more attractive—and in early 2025, perhaps the most significant remaining private constraint disappeared.

Google had prohibited fingerprinting in its advertising products since at least 2019. Announcing its Privacy Sandbox initiative that year, Google wrote: "Unlike cookies, users cannot clear their fingerprint, and therefore cannot control how their information is collected. We think this subverts user choice and is wrong."[5]

In December 2024, Google reversed course. Effective February 2025, Google's advertising products allowed fingerprinting, citing advances in privacy-enhancing technologies as a justification for a less prescriptive approach.[6]

The UK Information Commissioner's Office (ICO) called the decision "irresponsible," noting that Google's own prior statements showed the company understood fingerprinting's privacy implications.[7]

How We Got Here: The Cookie's Unintended Legacy

In June 1994, Lou Montulli, a 23-year-old engineer at Netscape, invented the HTTP cookie to solve a simple problem: websites could not remember what users had added to their shopping carts across page loads. The design was deliberately privacy-protective. Montulli rejected proposals for a permanent browser identifier because, as he later explained, "we wanted to build a mechanism where you could be remembered by the websites that you wanted to remember you, and you could be anonymous when you wanted to be anonymous."[8]

The initial cookie's core limitation—each cookie could only be read by the domain that set it—was a feature, not a bug. A cookie from *store.com* could only be read by *store.com*.

Within two years, industry advertisers discovered a workaround. By serving ads from their own domains across thousands of publisher sites, ad networks could set and read cookies everywhere those ads appeared. Third-party cookies were born. "We didn't want cookies to be used as a general tracking mechanism," Montulli told the New York Times in 2001.[9]

Notice-and-consent regimes—requiring companies to disclose data practices, often through dense legalese to obtain users' "agreement"—were built around cookies: banners, browser settings, "clear site data" buttons. These mechanisms assumed that tracking happened through something stored on the user's device that users could, at least in principle, delete. Montulli predicted the next move. Disabling cookies, he observed, would simply push tracking to mechanisms users couldn't control. That prediction is coming true.

How Fingerprinting Works

Fingerprinting collects attributes from a user's browser or device and combines them into a unique or near-unique identifier. Common fingerprinting vectors[10] include:

- **Canvas fingerprinting.** A script draws text and shapes to an invisible HTML5 canvas element, then reads back the rendered pixels. Differences in fonts, graphics drivers, anti-aliasing, and GPU behavior cause devices to render images differently. The resulting pixel data, hashed, becomes an identifier.

---

[5] Google, "Building a more private web" (August 22, 2019), https://blog.google/products/chrome/building-a-more-private-web/.

[6] Google, "Updating our ads data policies for the evolving regulatory and technological landscape" (December 2024).

[7] UK Information Commissioner's Office, "Our response to Google's policy change on fingerprinting" (December 19, 2024), https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/12/our-response-to-google-s-policy-change-on-fingerprinting/.

[8] NPR Planet Money, "The Invention That Satisfies Your Cookie Cravings" (November 2022), https://www.npr.org/transcripts/1137657496.

[9] Digital Content Next, "To understand where the cookie is headed, let's look at its history" (November 2020), https://digitalcontentnext.org/blog/2020/11/16/to-understand-where-the-cookie-is-headed-lets-look-at-its-history/

[10] Keaton Mowery & Hovav Shacham, "Pixel Perfect: Fingerprinting Canvas in HTML5" (2012), UC San Diego, https://hovav.net/ucsd/dist/canvas.pdf; Steven Englehardt & Arvind Narayanan, "Online Tracking: A 1-million-site Measurement and Analysis" (2016), ACM CCS, https://www.cs.princeton.edu/~arvindn/publications/OpenWPM_1_million_site_tracking_measurement.pdf

- **Audio fingerprinting.** A script processes an audio signal through the device's audio stack. Variations in how different devices handle audio processing produce unique signatures.
- **WebGL fingerprinting.** Queries about the graphics card, driver version, and rendering capabilities.
- **Font enumeration.** The set of fonts installed on a device is surprisingly distinctive—which can be shaped by the operating system, language preferences, installed software and user customization.
- **Navigator and screen properties.** Basic browser and device attributes such as screen resolution, color depth, timezone, language settings, and platform.

Individually, few of these attributes are unique. Combined, they produce identifiers that can distinguish most browsers. The Electronic Frontier Foundation's *Cover Your Tracks* project found that 83.6% of browsers had unique fingerprints.[11] Academic research confirms that fingerprints remain highly distinctive.[12]

Who Provides Fingerprinting Technology?

Several categories of companies develop and deploy fingerprinting technology. The boundaries between categories are porous; many firms operate across multiple segments.

Mobile measurement and attribution platforms. These companies provide Software Development Kits (SDKs) that app developers integrate to track advertising effectiveness. When device advertising identifiers (like Apple's IDFA) are unavailable, these platforms fall back to "probabilistic attribution"—fingerprinting by another name. Major providers include Adjust (owned by AppLovin), AppsFlyer, Branch, Kochava, and Singular.[13]

Browser fingerprinting services. Companies like Fingerprint (formerly FingerprintJS) offer fingerprinting as a primary product, marketing it for fraud detection and identity verification. Fingerprint claims 99.5% identification accuracy and emphasizes that its identifiers persist even when users clear cookies or use VPNs.[14]

Fraud detection and identity platforms. ThreatMetrix (owned by LexisNexis Risk Solutions) combines fingerprinting with behavioral analytics, operating what it calls the "Digital Identity Network" to track devices across thousands of client websites.[15] Kount (owned by Equifax) offers similar capabilities.

How Fingerprinting Works in Practice

Most fingerprinting reaches users through software development kits integrated into apps and websites. For example, a consumer-facing app developer may integrate an advertising SDK to monetize through ads; that SDK, running within the app, collects device attributes and transmits them to the SDK provider's servers.

AppLovin. AppLovin operates one of the largest mobile advertising platforms. Its SDK collects extensive device attributes, including battery levels, disk memory usage, and accessibility features.[16] In October 2025, the SEC's Cyber and Emerging Technologies Unit opened an investigation into AppLovin following whistleblower complaints alleging that the company's "AXON" platform engaged in systematic

---

[11] Electronic Frontier Foundation, Cover Your Tracks, https://coveryourtracks.eff.org/

[12] Gómez-Boix et al., "Hiding in the Crowd: an Analysis of the Effectiveness of Browser Fingerprinting at Large Scale" (2018), WWW Conference, https://dl.acm.org/doi/fullHtml/10.1145/3178876.3186097; "How Unique is Whose Web Browser? The role of demographics in browser fingerprinting among US users" (2024), https://arxiv.org/html/2410.06954v3.

[13] For an overview of mobile measurement platforms and probabilistic attribution, see Google Ads Help, "About tracking app conversions with an App Attribution Partner" https://support.google.com/google-ads/answer/12961402.

[14] Fingerprint, "Introduction to Fingerprint," https://dev.fingerprint.com/docs/introduction; FingerprintJS press release (November 2021). https://www.prnewswire.com/news-releases/fingerprintjs-raises-32m-to-empower-developers-to-combat-online-fraud-301415570.html.

[15] LexisNexis Risk Solutions, "ThreatMetrix,' https://risk.lexisnexis.com/products/threatmetrix.

[16] AppLovin Privacy Policy, https://www.applovin.com/privacy/; https://blog.applovin.com/blog/how-we-drive-value-and-handle-data/.

"identifier bridging" to circumvent platform privacy rules.[17] The investigation explores whether AppLovin harvested proprietary user identifiers from partners like Meta and Google to create unified digital profiles—or "Platform Identifier Groups"—that effectively nullify user-facing privacy controls.

The Tiny Lab litigation. In 2018, the New Mexico Attorney General sued Tiny Lab Productions along with Google and several ad-tech companies.[18] The complaint alleged that SDKs embedded in children's games collected persistent identifiers, including device fingerprints, without parental consent, violating COPPA. This litigation established that when SDKs collect persistent identifiers from children's apps, liability can attach if the operator has actual knowledge of the child-directed context.[19]

Why Fingerprinting is Spreading

The rise of fingerprinting reflects a structural shift in the data economy. Cookies gave platform operators—Google, Apple, Meta—control over user identity. Fingerprinting routes around these gatekeepers.

The "Bridging" Problem. While fingerprinting is often described as "probabilistic," the industry has moved toward "Identifier Bridging" that stitches a device fingerprint to a stable identifier like a hashed email address. When a user logs into an app, the SDK captures the email and the fingerprint simultaneously. The provider then "bridges" the two. This linkage means that even if the user later browses in "incognito mode", the provider or a third party data broker can immediately re-attach their real identity. Bridging converts what might otherwise be a weak probabilistic match into a durable, cross-context identifier, effectively recreating cookie-style tracking without meaningful user control.

The Connected TV (CTV) Driver. Smart TVs (Roku, Samsung, Vizio) never supported cookies and, as a result, the CTV ad market is built almost entirely on fingerprinting and bridging. A substantial and growing share of fingerprinting-based ad bidding now originates from CTV environments, where users have almost zero visibility into how their viewing habits are being linked to their mobile devices.[20]

IP Masking and Signal Shifting. As IP addresses have historically been among the strongest signals for identification, the growing adoption of IP masking—through browser features, VPNs, and relay services—is shifting the fingerprinting landscape. This pushes companies toward other device attributes and accelerates the move to bridging techniques that rely on authenticated identifiers rather than network-level signals.

Existing Consent Mechanisms

The cookie consent regime is built around the assumption that tracking happened through client-side storage—that is, on a user's device. Fingerprinting breaks that assumption. Cookie banners ask users to accept or reject cookies, but fingerprinting does not rely on storing anything on the device. The website can recognize your device by its existing features—like noticing the dents, paint color, or accessories on a car. Thus, websites can identify a device by observing its built-in hardware characteristics, and that identifier is created and kept on the company's servers without any moment where a user would be offered a "notice and consent" pop-up.

The ICO's "Access" Theory. In early 2025, the UK ICO finalized guidance clarifying that fingerprinting is subject to the same consent requirements as cookie-setting under the ePrivacy Directive. Their reasoning is that the law applies to any technology

---

[17] Bloomberg, "AppLovin Faces SEC Probe Over Data Practices" (October 6, 2025), https://www.bloomberg.com/news/articles/2025-10-06/applovin-has-been-probed-by-sec-over-data-collection-practices.

[18] New Mexico Department of Justice, "AG Balderas Announces Lawsuit Against Tech Giants Who Illegally Monitor Child Location, Personal Data" (September 2018), https://nmdoj.gov/press-release/ag-balderas-announces-lawsuit-against-tech-giants-who-illegally-monitor-child-location-personal-data/

[19] Balderas v. Google LLC, settlement announced August 2021; see MediaPost, "Google And New Mexico Reach Settlement Over Children's Privacy" (August 2021), https://www.mediapost.com/publications/article/366186/google-and-new-mexico-reach-settlement-over-childr.html

[20] For background on CTV advertising and identity resolution, see IAB Tech Lab, "Identifier for Advertising (IFA) Guidelines," https://iabtechlab.com/standards/guidelines-for-identifier-for-advertising-ifa-for-ctv/

that "accesses information already stored on a user's terminal equipment." Since a fingerprinting script must "access" the device's hardware specs to function, explicit consent is required, regardless of whether a physical "cookie" is dropped.[21]

Global Privacy Control. GPC is a legally recognized opt-out signal under certain state privacy laws. California regulations require covered businesses to honor GPC as a valid opt-out request.[22] But GPC assumes the existence of a technical mechanism the site can actually disable. It works for cookies: the site can simply stop setting them. It should work the same way for fingerprinting, although compliance is harder to observe because fingerprinting data is collected server-side.

Harms

Fingerprinting operates based on the premise that it is unavoidable and opaque to the user. First, there is no meaningful opt-out. Users cannot prevent fingerprinting through any available control mechanism. Second, fingerprinting is difficult to detect. Users cannot see it happening, and even developers may not understand precisely what the SDKs they integrate are collecting.

As a result, fingerprinting practices give rise to several concrete harms:

Circumvention of Consumer Choice. Fingerprinting represents a fundamental subversion of consumer autonomy. When a user engages with platform-level controls—such as selecting "Ask App Not to Track" on iOS or enabling a Global Privacy Control (GPC) signal—they are making an explicit choice to opt out of the data economy. Fingerprinting renders these choices a nullity. By utilizing "active" signals that route around these headers and settings, companies engage in what may be characterized as deceptive and unfair trade practices. They provide the illusion of control while maintaining a persistent, invisible tether to the user's identity, effectively treating a "no" as a "yes."

Re-identification. Fingerprinting can link activity that users believed was private, such as browsing in incognito mode, clearing cookies, or visiting sites without logging in. Actions that users believed were separate can be linked together.

Discriminatory applications. Persistent identifiers enable surveillance pricing and targeting based on inferred characteristics such as income, education, health status, or vulnerability. These inferences are often drawn without user knowledge and may result in discriminatory outcomes.[23]

Investigating Fingerprinting

Demonstration tools. Tools like the EFF's *Cover Your Tracks* let users see their own browser fingerprint, informing investigations by showing what data is collected.[24]

To learn more about a company's practices, here are some open questions that could be posed to firms:

- **Technical implementation evidence.** SDK documentation and data dictionaries showing "probabilistic identifiers," "persistent identifiers," "cookieless tracking," or "fingerprints".
- **Identity and linking evidence.** Metrics for "Probabilistic-to-Deterministic Lift" (showing how many anonymous fingerprints were linked to real emails).
- **Cross-context identity infrastructure.** The existence of an "ID Graph" where various identifiers are stitched together.

---

[21] UK Information Commissioner's Office, "Guidance on the use of cookies and similar technologies" (2025); see also ICO statement on fingerprinting (December 2024), https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/12/our-response-to-google-s-policy-change-on-fingerprinting/.

[22] California Attorney General, "Making Your Business CCPA Compliant: Global Privacy Control," https://oag.ca.gov/privacy/ccpa/gpc; see also Global Privacy Control specification, https://globalprivacycontrol.org/.

[23] For research on demographic disparities in fingerprinting exposure, see "How Unique is Whose Web Browser? The role of demographics in browser fingerprinting among US users" (2024), https://arxiv.org/html/2410.06954v3.

[24] Electronic Frontier Foundation, Cover Your Tracks, https://coveryourtracks.eff.org/; see also AmIUnique, https://amiunique.org/.

- **Terminology signaling fingerprinting or identity expansion.** Terms like “Identifier Bridging,” “Cross-Platform Matching,” or “Hashed Email Enrichment”.
- **Consent circumvention evidence.** Communications about maintaining identity persistence when cookies are blocked.
- **Vendor and third-party involvement.** Identify all third-parties, SDKs, or service providers involved in fraud detection, analytics, advertising, targeting or personalization.
- **Use cases and downstream effects.** Identify all purposes that fingerprinting is used including: advertising, targeting, personalization, A/B testing —and state whether those identifiers are used to modify prices, offers, or defaults, recognize repeat visitors, target messaging or urgency cues.
- **Internal knowledge, process, and intent.** Any internal documents discussing “cookie deprecation,” “fingerprinting,” “device recognition,” or any analyses addressing fingerprinting or similar techniques.
- **Device and user recognition.** How does the company recognize or distinguish repeat users or devices across sessions?
- **Data collection for identification.** What device, browser or system attributes are collected (e.g. fonts, screen properties, performance data).
- **Fingerprinting methods.** Do you generate identifiers from combinations of device attributes?
- **Identity persistence beyond cookies.** How do you maintain user identity across sessions when cookies are cleared?
- **Purpose limitation.** Do you use the same identifiers for fraud detection and for advertising?
- **Effectiveness of user opt-outs.** If you offer opt-out mechanisms, how do they affect fingerprint-based tracking?
- **Identity linking and expansion.** Do you engage in “identifier bridging” or link probabilistic identifiers to authenticated user data?

Conclusion

Device fingerprinting is a long-established technique that is finding new life today. As third-party cookies are deprecated, the economic incentive to fingerprint has never been stronger. The technique is well understood, and the harms are concrete: loss of user control, opacity, and the creation of inescapable digital profiles.

The current landscape—marked by Google’s policy reversal and the rise of identifier bridging—demands new scrutiny from enforcers. Fingerprinting that lacks meaningful disclosure raises serious concerns under consumer protection and privacy statutes. Where laws require purpose limitations, the dual-use nature of fingerprinting technology using fraud detection to justify data collection that also enables advertising may require additional attention.

CITP

CITP.PRINCETON.EDU

The Center for Information Technology Policy
Princeton University / 303 Sherrerd Hall
Princeton, NJ 08544 /citp@princeton.edu

AUTHORS

Adam Pickersgill CITP Non-Resident Technology Fellow

Patrick Yurky Institute for Technology Law & Policy, Georgetown Law

Varun Gadh CITP Non-Resident Technology Fellow

Stephanie T. Nguyen Senior Fellow, Columbia Law School

Mihir Kshirsagar Clinic Lead and CITP Steering Committee Member

COLLABORATORS

INSTITUTE FOR
TECHNOLOGY
LAW & POLICY
GEORGETOWN LAW