INSIGHT REPORT

DIGITAL 520

Why Third-Party Tracking Is Being Eliminated, How It Works, and What Replaces It

A Technical and Privacy Guide to the End of Cross-Site Behavioral Tracking, for Engineering Teams, Business Leaders, and Everyone Who Depends on the Open Web

PREPARED BY	Noah M. Kenney, Principal Consultant
DATE	March 2026

Table of Contents

Executive Summary

Third-party cookies are small text files that have underpinned cross-site behavioral tracking for more than two decades. They are being systematically eliminated, not because the industry chose to move on, but because regulators, browser vendors, and courts decided the privacy tradeoffs were no longer acceptable. Understanding why they are disappearing, how they worked in the first place, and what technical mechanisms are replacing them is now a required competency for any organization with a digital presence.

This report is organized around three questions:

1) How did third-party cookies enable the tracking ecosystem that now exists?
2) What specific technical and regulatory forces are dismantling that ecosystem?
3) And what replaces it, both technically and from a user privacy standpoint?

The answers reveal a system whose privacy implications were largely invisible to the users it profiled. A typical web session generates dozens of tracking calls to ad networks, data brokers, and analytics platforms, none of which the user deliberately engaged with. Browsers and operating systems are responding with enforcement mechanisms that make cross-site behavioral profiling technically impossible without user consent, a change that is both technically significant and, for most users, genuinely positive.

Key Takeaway

The end of third-party cookies is not primarily a business transition: it is a privacy correction. The technical alternatives that replace them are architecturally different in ways that matter: they move data processing closer to the user, reduce the surface area for data leakage, and make tracking harder to do invisibly. Organizations that understand these architectural differences will make better decisions about compliance, user trust, and long-term data strategy.

~300	25%	7 yrs	95+
Avg. third-party tracking calls per web session before browser enforcement[1]	iOS ATT opt-in rate, revealing actual user consent levels for behavioral tracking[2]	Time span from Safari ITP (2017) to Google Chrome user-choice rollout (2024)[3]	Countries with comprehensive data privacy legislation in force as of 2025[4]

Sources: [1] Princeton Web Transparency and Accountability Project; [2] Flurry/Yahoo industry estimates; [3] Browser release notes and Google Privacy Sandbox timeline; [4] IAPP Global Privacy Law and DPA Directory.

Scope & Objectives

This report addresses three objectives:

- **Explain the technology.** Provide a technically accurate account of how third-party cookies enable cross-site tracking, including the HTTP mechanisms, the ad tech stack that uses them, and the specific privacy harms they create.
- **Document the deprecation.** Trace the multi-year process by which browser vendors, mobile operating systems, and regulatory bodies dismantled cookie-based tracking, and clarify what has actually changed as of early 2026.
- **Assess the replacements.** Evaluate the technical alternatives being deployed in the post-cookie environment, their capabilities, their genuine privacy properties, and their limitations, so that organizations can make informed implementation decisions.

Part I: How Third-Party Cookies Work — and Why They're a Privacy Problem

To understand why third-party cookies are being eliminated, you first need to understand what they are, how they function at a protocol level, and what they made possible at scale. The privacy problem is architectural: it was not an accident or an abuse of the system, but a consequence of what the system was designed to do.

The Cookie Protocol: A Technical Primer

A cookie is a small key-value data store set by a server and persisted in the user's browser. When a server includes a Set-Cookie header in an HTTP response, the browser stores it and returns it in the Cookie header of every subsequent request to that domain. This mechanism was introduced in 1994 by Lou Montulli at Netscape as a way to implement session state in an otherwise stateless HTTP protocol.[5]

> ### Technical Detail: Cookie Mechanics
>
> A first-party cookie is set by the domain the user is currently visiting. If you visit example.com, the Set-Cookie response header from example.com creates a first-party cookie that is returned to example.com on every subsequent visit.
>
> A third-party cookie is set by a different domain, one whose resources are embedded in the page you're visiting. If example.com loads an image from adnetwork.com, adnetwork.com can set a cookie on your browser through its Set-Cookie response header. That same cookie will be sent back to adnetwork.com every time you visit any other site that also loads adnetwork.com resources, enabling adnetwork.com to recognize you across unrelated websites.
>
> The key attribute that enables cross-site tracking is persistence: unlike session cookies (which expire when the browser closes), tracking cookies are typically set with a far-future Expires or Max-Age attribute, allowing them to persist for months or years.

The SameSite cookie attribute, introduced in 2016 and strengthened in 2020, was the first major technical countermeasure. It controls whether cookies are sent on cross-site requests. Cookies with SameSite=Strict are never sent on cross-site requests. Cookies with SameSite=Lax are sent only on top-level navigations. Cookies with SameSite=None (the legacy default for third-party cookies) are sent in all contexts, but Chrome began requiring these to also carry Secure=true in 2020.[6]

The Tracking Stack Explained

Third-party cookies became the foundation of a multi-layer data infrastructure. Understanding that infrastructure is essential to understanding what is actually being disrupted.

Layer	Technology	What Third-Party Cookies Enabled
Ad Networks & Exchanges	Google Ad Manager, OpenX, Xandr	Persistent user identifier across publisher inventory for frequency capping, retargeting, and cross-publisher reach measurement
Demand-Side Platforms (DSPs)	The Trade Desk, DV360, MediaMath	Bidding on impressions based on behavioral audience segments built from cross-site data
Data Management Platforms (DMPs)	Salesforce DMP, Oracle BlueKai	Aggregating cross-site behavioral data into audience segments sold to advertisers
Analytics Platforms	Google Analytics (Universal), Adobe Analytics	Cross-domain user journey tracking and attribution without authentication
Tag Managers	Google Tag Manager, Tealium	Deploying third-party pixel/cookie combinations at scale without engineering involvement
Identity Graphs	LiveRamp, Neustar, Experian	Linking browser cookie IDs to offline identity data (name, address, purchase history)

Table 1. The major layers of the third-party cookie tracking stack and their dependence on cross-site cookie identifiers. Source: Digital 520 Analysis.

The real-time bidding (RTB) auction that underlies most programmatic advertising depends on all of these layers functioning together. When a user loads a web page, the publisher's supply-side platform (SSP) broadcasts an auction opportunity that includes the user's cookie-based ID. Each demand-side platform queries its audience databases, populated with data from DMPs, identity graphs, and cross-site behavioral history, and submits a bid. The entire system depends on a persistent, shared identifier: the third-party cookie.[7]

> **The Scale of Invisible Tracking**
>
> Research from Princeton's Web Transparency and Accountability Project found that a majority of the top 1 million websites load third-party tracking code from Google, Meta, or both. On a typical news or retail site, a user's browser makes 50-300 third-party requests per page load, each of which may set or read cookies. The user has no visibility into this activity, and in most jurisdictions prior to GDPR, no mechanism to opt out.

Privacy Violations by Design

The privacy implications of third-party cookie infrastructure operate on several levels. The least visible, and arguably the most significant, is the construction of persistent behavioral profiles without meaningful user awareness or consent.

- **Cross-site behavioral profiling.** An ad network embedded in thousands of publisher sites can observe and record every page a user visits that includes its tracking pixel. Over time this creates a detailed behavioral profile: political interests inferred from news sites visited, health conditions inferred from medical content, financial situation inferred from investment or loan-related searches. None of this data is directly provided by the user.

- **Re-identification of supposedly anonymous data.** Cookie-based profiles can be linked to real identity through a process called cookie syncing, in which two ad networks exchange cookie IDs and link their respective behavioral datasets. Once linked, an identifier that appeared anonymous can be connected to a known identity if either party has authenticated user data (such as an email address from a login).
- **Data persistence and breadth.** Unlike data a user consciously provides to a service, cookie-based behavioral data persists across sessions, across devices (through probabilistic fingerprinting or cross-device matching), and can be sold or licensed to parties the user never interacted with. Data brokers built multi-billion dollar businesses on this supply chain.
- **Lack of meaningful consent.** Prior to GDPR, most third-party tracking required no user notification. The consent mechanisms that emerged after GDPR, cookie banners, are widely criticized as dark-pattern implementations that make refusal intentionally difficult. Research by the Norwegian Consumer Council found that the majority of cookie consent frameworks were designed to nudge users toward acceptance rather than provide genuine choice.

> ### Technical Note: Cookie Syncing
>
> Cookie syncing is the mechanism by which two independent ad networks share user identifiers. Network A embeds a pixel on a page and sets its own cookie ID. Network B's pixel is also present. Network A calls a redirect URL on Network B, appending its own user ID as a URL parameter. Network B reads its own cookie for the same browser, links the two IDs, and responds. The result is a shared cross-network identifier.
>
> This process happens silently on millions of page loads and is invisible to users. It is the technical mechanism that enabled "audience extension" products, allowing an advertiser's first-party audience data to be matched against third-party behavioral data at scale.

The Regulatory Response

The regulatory response to cookie-based tracking built over a decade. It accelerated sharply after a series of high-profile data scandals demonstrated the real-world consequences of unconstrained behavioral data collection.

Regulation	Jurisdiction	Key Cookie/Tracking Provisions
ePrivacy Directive (2002, amended 2009)	European Union	First EU law requiring consent for storing information on user's device. Widely unenforced due to lack of implementing regulations.

Regulation	Jurisdiction	Key Cookie/Tracking Provisions
General Data Protection Regulation (GDPR, 2018)	European Union	Requires freely given, specific, informed, and unambiguous consent for processing personal data. Applies to cookie-based identifiers as personal data. Enforced by national DPAs with fines up to 4% of global revenue.
California Consumer Privacy Act (CCPA, 2020)	California, USA	Grants consumers right to opt out of sale of personal information, which includes behavioral data derived from cookie tracking. Amended by CPRA (2023) to add right to limit use of sensitive personal information.
Digital Markets Act (DMA, 2023)	European Union	Requires "gatekeepers" (Google, Meta, Apple) to obtain separate consent before combining personal data across services. Directly attacks cross-service identity infrastructure.
UK GDPR / Data Protection Act 2018	United Kingdom	Post-Brexit equivalent of EU GDPR. ICO guidance specifies that cookie-based identifiers constitute personal data and require valid consent under legitimate interest or consent lawful basis.

Table 2. Key privacy regulations and their specific implications for cookie-based tracking infrastructure. Source: Digital 520 Analysis.

The most significant enforcement actions came from the French CNIL, which fined Google €150 million and Meta €60 million in January 2022 for making it harder to refuse cookies than to accept them. The Irish DPC's enforcement decisions against Meta on cross-service data combination are ongoing. In the United States, the FTC's enforcement actions against data brokers and the state-level privacy law expansion (currently 20+ states with comprehensive privacy laws) are creating a similar compliance pressure.[10,11]

Part II: The Deprecation Timeline — What Changed and When

The end of third-party cookies did not happen all at once. It has been a multi-front process spanning nearly a decade, driven independently by browser vendors, mobile platform owners, and regulators. Understanding the timeline matters because different parts of the tracking infrastructure were dismantled at different times, and the disruption has been uneven across channels.

Safari's Intelligent Tracking Prevention (2017–2020)

Apple's WebKit team shipped Intelligent Tracking Prevention (ITP) in Safari in September 2017. ITP version 1.0 used machine learning to classify third-party domains as tracking domains based on their cross-site presence. Cookies from classified domains were partitioned to prevent cross-site access. This was the first major browser-level countermeasure against third-party tracking.[12]

> ### ⚙ How ITP Works Technically
>
> ITP uses a classifier that evaluates whether a domain has been observed making resources available across multiple top-level domains in a way consistent with tracking behavior. Domains classified as tracking domains have their cookies placed in a separate partition, they can be read when the user directly navigates to that domain (first-party context), but not in third-party contexts.
>
> ITP 2.0 (2018) extended this to block all third-party cookies from classified tracking domains entirely. ITP 2.1 (2019) added a 7-day cap on all script-writeable first-party storage (localStorage, sessionStorage, and IndexedDB) set via third-party scripts, limiting fingerprinting workarounds. ITP 2.3 (2019) closed the cross-site link decoration workaround by stripping tracking parameters from URLs.

The practical impact was significant: Safari held approximately 20-25% of global browser market share, meaning roughly a quarter of web users were no longer trackable via third-party cookies in Safari. The advertising industry responded with workarounds, link decoration (appending user IDs to URLs), CNAME cloaking (routing third-party requests through first-party subdomains), and fingerprinting. Apple progressively closed each workaround in subsequent ITP iterations.[13]

Apple's App Tracking Transparency (2021)

In April 2021, Apple shipped iOS 14.5 with the App Tracking Transparency (ATT) framework. ATT requires all iOS apps to explicitly request user permission before accessing the device's IDFA (Identifier for Advertisers), the mobile equivalent of a third-party cookie. The permission prompt is unambiguous: "Allow [App] to track your activity across other companies' apps and websites?"[2]

The result was revealing. Opt-in rates globally settled at approximately 25%, meaning three in four users denied permission when asked directly and clearly. This data point is significant not just for what it did to ad performance, but for what it revealed about actual user preferences when consent was genuinely informed and freely given.

What ATT Revealed About Consent

Prior to ATT, mobile app tracking was opt-out by default: the IDFA was available to all apps unless the user navigated to Settings > Privacy > Tracking to disable it. Very few users did. When Apple changed the default to opt-in with a clear prompt, 75% of users said no. This gap between "default-on" and "genuinely-asked" consent rates is the most important data point in the privacy debate: users are not indifferent to tracking, they simply had no meaningful mechanism to express that preference.

Google's Privacy Sandbox: A Platform Redesign (2019–2026)

Google announced the Privacy Sandbox initiative in August 2019, proposing to replace third-party cookies in Chrome with a set of privacy-preserving APIs. The initiative was framed as a way to preserve advertising functionality while eliminating the most invasive privacy characteristics of third-party cookies. Its technical design choices reflect the fundamental tension between these goals.[14]

Google originally proposed to deprecate third-party cookies in Chrome by late 2022. The deadline was extended five times, ultimately to 2024. Google then revised its approach: rather than deprecating third-party cookies entirely, Chrome now presents users with a one-time choice about whether to enable third-party cookies. This change was driven by pressure from the UK Competition and Markets Authority (CMA), which was investigating whether Google's cookie deprecation would unfairly advantage its own advertising products.[15]

API / Proposal	Purpose	Technical Approach	Current Status (2026)
Topics API	Interest-based targeting without cross-site profiles	Browser observes user's browsing, assigns weekly interest topics from a public taxonomy (~350 topics). Advertisers can query up to 3 topics per impression. No individual site history exposed.	Shipping in Chrome. Adoption limited by publisher and DSP integration gaps.
Protected Audience API (formerly FLEDGE)	Retargeting without third-party cookie syncing	Advertiser adds user to interest group directly in browser. Auction runs on-device in an isolated JavaScript worklet. Winning ad is rendered in a fenced frame.	Shipping in Chrome. Functionally limited compared to server-side retargeting. Adoption growing slowly.
Attribution Reporting API	Conversion measurement without cross-site identity	Browser matches ad impression to conversion and generates a privacy-preserving aggregate report with noise added. No individual-level attribution data exposed.	Shipping in Chrome. Replacing some use cases for the deprecated third-party cookie conversion pixel.

API / Proposal	Purpose	Technical Approach	Current Status (2026)
Storage Access API	Allowing embedded third parties to request first-party storage access	Third-party iframes can request access to their own first-party cookies via a user-prompted permission dialog. Useful for authenticated embeds (logins, widgets).	Shipping in Chrome, Safari, and Firefox. Primary use case: SSO and authenticated embeds.
Chips (Partitioned Cookies)	Allowing cookies that are scoped to the top-level site	Third-party cookies with the Partitioned attribute are scoped to the specific first-party context, preventing cross-site tracking while allowing functional embeds (widget state, cart persistence on embedded storefronts).	Shipping in Chrome 114+. Addresses embedded functionality use cases without enabling tracking.

Table 3. Google Privacy Sandbox API overview, technical approach, and deployment status as of early 2026. Source: Digital 520 Analysis based on Google Privacy Sandbox documentation.

Where Things Stand in 2026

The net result of the deprecation timeline is a fragmented landscape rather than a clean transition:

- **Safari and Firefox:** Third-party cookies have been blocked by default since 2020 and 2019, respectively. Combined these browsers represent approximately 30-35% of global web traffic.
- **Chrome:** Third-party cookies remain available but users have been presented with a one-time consent choice. Estimates suggest 40-60% of Chrome users will disable third-party cookies when prompted, though the actual rollout and opt-out rates are still being measured.
- **iOS App Tracking:** The IDFA is unavailable for approximately 75% of iOS users. Equivalent opt-in rates on Android are lower but growing as Google's Privacy Sandbox for Android evolves.
- **Privacy Sandbox APIs:** Deployed in Chrome but adoption is uneven. Most DSPs and publishers have partial integration. The APIs do not provide equivalent functionality to third-party cookies for all use cases, particularly cross-site retargeting and individual-level attribution.

Part III: Technical Alternatives to Third-Party Cookies

No single technology replaces third-party cookies. The ecosystem is replacing a general-purpose cross-site identifier with a set of purpose-specific, architecturally constrained tools. Understanding the differences matters because the constraints are not just technical limitations, they are the privacy properties. Each alternative's design reflects a different set of tradeoffs between tracking capability and user privacy.

Google Privacy Sandbox APIs

The Privacy Sandbox APIs are browser-native alternatives to specific third-party cookie use cases. They are designed to limit the data available to any individual party while preserving some advertising functionality. Their key architectural innovation is moving processing from servers, where data can be freely collected and combined, to the browser, where it can be restricted and audited.

Topics API

The Topics API assigns users to interest categories (topics) based on browsing history observed by the browser. When an ad auction occurs, the API provides up to three topics relevant to the user's recent interests, drawn from the current week and two prior weeks. Topics are drawn from a public taxonomy of approximately 350 categories. The API does not expose which sites the user visited, and each topic is only shared with a site if that site was also observed in relation to that topic.[17]

> ⚙ **Technical Constraints of the Topics API**
>
> Topics are limited to a predefined public taxonomy: no custom audiences or fine-grained behavioral segments.
>
> A maximum of 3 topics are returned per call, and the topic for the calling domain is only returned if that domain has itself observed the topic for that user.
>
> Topic epochs rotate weekly, limiting the accumulation of persistent profiles.
>
> The API includes a noise mechanism: 5% of the time, a random topic is returned instead of an observed one.
>
> Privacy limitation: While significantly more constrained than cookie-based profiling, Topics API data can still be used to infer sensitive categories (health, politics) depending on the topic taxonomy.

Protected Audience API

Protected Audience (formerly FLEDGE) addresses the retargeting use case, showing users ads related to sites or products they have previously visited. In the third-party cookie model, this worked by syncing the user's cookie ID between the advertiser's DMP and the ad network, then bidding against that ID in real-time auctions. Protected Audience moves the entire mechanism into the browser.[18]

The advertiser calls the browser's joinAdInterestGroup() API directly, placing the user in a named interest group stored in the browser. When an auction runs, the browser executes bidding logic (provided by the advertiser as a JavaScript function) in an isolated worklet, a sandboxed execution environment with no network access. The winning ad is rendered in a fenced frame that cannot communicate with the surrounding page.

> ⚙ **Protected Audience Architecture**
>
> Interest groups are stored in the browser, not on any server; they cannot be read by third parties or cross-matched with other data.
>
> Bidding functions run in isolated JavaScript worklets with no network access during the auction, preventing real-time data exfiltration.
>
> Fenced frames prevent the winning ad from communicating with the embedding page or learning which site rendered it.
>
> The auction result and winning creative are subject to k-anonymity requirements: an ad can only be shown if it would be shown to at least k users (k=50 in current implementation), preventing micro-targeted creatives.
>
> Limitation: On-device auctions are computationally constrained compared to server-side alternatives. Complex ML-based bidding strategies cannot run in browser worklets.

Attribution Reporting API

Third-party cookies were widely used for conversion attribution: when a user clicked an ad and then converted on the advertiser's site, a cookie ID linked the click event to the conversion. The Attribution Reporting API provides a privacy-preserving alternative that does not require a shared cross-site identifier.[19]

The API registers ad impressions and clicks in the browser. When a conversion occurs, the browser generates an attribution report and queues it for delivery with a variable delay (up to 24 hours, with noise). Event-level reports provide limited data (click ID, basic conversion metadata). Aggregate reports use differential privacy techniques, adding statistical noise, to prevent individual-level inference. No individual user's conversion path is ever exposed.

First-Party Data Infrastructure

The highest-value investment in the post-cookie environment is first-party data: data collected directly from users through owned channels, with explicit consent. First-party data is not subject to browser-level restrictions because it exists within a single domain context, and it is inherently higher quality because it reflects direct user relationships rather than inferred behavioral profiles.

Building genuine first-party data infrastructure typically requires several technical components:

- **Identity resolution layer.** A system that links authenticated users (logged-in sessions) across devices and sessions using email-based or phone-based identifiers. Unlike cookie-based cross-device matching, authenticated identity resolution is deterministic rather than probabilistic.

- **Consent management platform (CMP).** A system for recording, storing, and honoring user consent choices in a way that is technically enforceable and legally auditable. CMPs that comply with the IAB TCF (Transparency and Consent Framework) v2.2 are the current industry standard for GDPR compliance.
- **Customer data platform (CDP).** A unified database that aggregates first-party data from web, app, CRM, and offline sources into persistent customer profiles that can be used for segmentation, personalization, and activation.
- **Server-side event tracking.** Sending conversion and behavioral events directly from the advertiser's server to ad platforms' Conversion APIs, bypassing the browser entirely and avoiding both cookie limitations and ad blocker interference.

Server-Side Tracking

Server-side tracking routes user event data through the advertiser's own server before forwarding it to advertising and analytics platforms, rather than firing client-side pixels directly from the user's browser. This approach is increasingly important because browser-based tracking is subject to ITP, browser extensions, and other client-side restrictions, while server-side requests originate from the advertiser's infrastructure and are not restricted by these mechanisms.

> ### Server-Side Tracking Architecture
>
> User takes an action (page view, add to cart, purchase) on the advertiser's site. The browser fires a standard event to the advertiser's own server-side endpoint (same domain, therefore a first-party request).
>
> The advertiser's server enriches the event with data from its own systems (CRM data, order information, authenticated user ID) and forwards it to platform Conversion APIs (Meta CAPI, Google Ads Conversion API, TikTok Events API).
>
> The result is a conversion event attributed to a specific ad interaction using platform-side matching (hashed email, phone number, user agent) rather than a cross-site cookie.
>
> Privacy consideration: Server-side tracking does not inherently improve user privacy: it moves the tracking infrastructure to a place where users have less visibility. Its privacy properties depend entirely on the organization's data handling practices and whether appropriate consent has been obtained.
>
> Compliance consideration: Under GDPR, server-side tracking still constitutes processing of personal data if it involves identifiable users. Consent requirements apply regardless of whether tracking is client-side or server-side.

Contextual Targeting

Contextual targeting serves ads based on the content of the page being viewed rather than the behavioral history of the user viewing it. It is the oldest form of digital advertising and the one most resistant to the privacy-related changes in the ecosystem, since it requires no individual user data at all.

Modern contextual targeting has advanced substantially beyond simple keyword matching. Natural language processing (NLP) models can classify page content across hundreds of topic and sentiment dimensions, enabling targeting at a level of sophistication that approaches behavioral targeting for categories where purchase intent is strongly correlated with content consumption (automotive, travel, financial services).

From a privacy standpoint, contextual targeting has genuine advantages: it does not build or require user profiles, it generates no cross-site tracking data, it requires no consent under GDPR (since it does not process personal data), and it provides no mechanism for user re-identification. For organizations seeking both compliance simplicity and user trust, contextual is the structurally clean choice.

Identity Solutions: UID2, ATS, and PPIDs

Several industry initiatives have developed authenticated identity frameworks that replace the cross-site cookie ID with an identifier derived from authenticated user data, typically a hashed email address or phone number. These solutions maintain some cross-site targeting capability while shifting from behavioral observation to authenticated consent.[20]

Solution	Operator	Mechanism	Privacy Properties
Unified ID 2.0 (UID2)	The Trade Desk (open-source)	Hashed and encrypted email/phone submitted at authentication. Hash is shared across participating publishers and DSPs. User can opt out via global opt-out endpoint.	Depends on user awareness that authentication creates a trackable ID. Coverage limited to authenticated environments. Opt-out mechanism exists but discovery is low.
LiveRamp ATS (Authenticated Traffic Solution)	LiveRamp	Publisher authenticates user (email at login); LiveRamp generates an encrypted RampID for use in ad auctions. Advertiser CRM data is matched server-side.	No direct cookie dependency. Requires explicit authentication. Data passes through LiveRamp infrastructure, not on-device. Subject to LiveRamp privacy policy and client agreements.
Google PPID (Publisher-Provided Identifiers)	Google	Publisher generates an opaque identifier for authenticated users and passes it to Google Ad Manager. Google uses it for frequency capping and targeting within Google's ecosystem only.	ID is opaque to Google; Google cannot reverse it to real identity. Only usable within Google ecosystem. Not a cross-DSP solution.

Solution	Operator	Mechanism	Privacy Properties
ID5	ID5 (independent)	Probabilistic and deterministic matching across publisher network. Builds a persistent ID from browser signals and authentication data where available.	Partially probabilistic, not all matches are consent-based. Privacy properties weaker than fully authenticated solutions. Subject to GDPR consent requirements.

Table 4. Identity solution comparison for post-cookie environments.
Source: Digital 520 Analysis.

Data Clean Rooms

A data clean room is a secure computing environment that allows two parties to analyze overlapping datasets without either party directly accessing the other's raw data. In the advertising context, clean rooms enable advertisers to match their first-party customer data against publisher audience data to measure campaign effectiveness, audience overlap, and reach, without either party exposing individual-level records.[21]

Clean Room Technical Architecture

An advertiser uploads a hashed version of its first-party customer list (e.g., CRM emails) to the clean room environment. A publisher uploads a hashed version of its authenticated audience.

The clean room executes queries over the overlapping dataset within an isolated compute environment. Differential privacy techniques add statistical noise to query results to prevent individual-level inference from aggregate outputs.

Neither party receives the other's raw data. The result is an aggregated match report (e.g., "17,000 users who saw this campaign were in the advertiser's CRM dataset") without either party being able to reconstruct the other's identity list.

Major implementations: Google Ads Data Hub, Meta Advanced Analytics, Amazon AWS Clean Rooms, Snowflake Secure Data Sharing, InfoSum.

Privacy properties: Clean rooms are significantly more privacy-protective than cookie syncing. However, differential privacy guarantees vary by implementation, and adversarial reconstruction attacks on insufficiently noised outputs remain a research concern.

Part IV: Privacy Implications

The transition away from third-party cookies produces genuine privacy improvements. But it also introduces new risks and leaves some fundamental privacy problems unresolved. An accurate assessment requires examining both what changes and what does not, and recognizing that "privacy-preserving" as a marketing term does not always mean what it implies architecturally.

What Users Actually Gain

Several things do genuinely improve for users as third-party cookies are eliminated and the Privacy Sandbox APIs deploy:

- **Reduced cross-site behavioral profiling.** The invisible accumulation of browsing behavior across thousands of unrelated sites, the core mechanism of third-party cookie tracking, becomes technically much harder. Without a shared identifier, ad networks cannot silently observe and link a user's activity across sites they did not choose to engage with.
- **Profile data stays in the browser.** Privacy Sandbox APIs like Topics and Protected Audience keep user interest data on the device rather than uploading it to servers. This is architecturally significant: data on a server can be breached, sold, or subpoenaed. Data in the browser is subject to none of those risks.
- **Consent becomes more meaningful.** ATT's 25% opt-in rate demonstrates that when consent is genuinely informed and easily exercised, a large majority of users choose to limit tracking. Regulatory enforcement is gradually moving cookie consent on the web in the same direction, closing the gap between "technically consented" (clicking accept on a dark-pattern banner) and genuinely consented.
- **Fewer data brokers in the loop.** Cookie-based data broker ecosystems depend on the ability to share user identifiers across companies. Browser-level partitioning and cookie blocking directly reduce the surface area of that sharing, shrinking the data supply chain that links behavioral observation to real-world identity.

What Still Threatens Privacy

Cookie deprecation does not solve privacy. Several significant tracking mechanisms either survive the transition or are strengthened by it:

- **Browser fingerprinting.** A browser can be identified through the combination of its user agent string, screen resolution, installed fonts, browser plugins, canvas rendering behavior, and WebGL rendering characteristics, without any cookies at all. Studies suggest that 80-95% of browser instances can be uniquely identified through fingerprinting. The elimination of cookies increases the relative importance of fingerprinting as a tracking technique.
- **Walled garden consolidation.** Google, Meta, and Amazon all operate closed ecosystems with authenticated users and first-party data at scale. The decline of open-web third-party cookies strengthens these platforms because they are the least affected, their tracking infrastructure is

first-party within their own ecosystems. Users who interact with Google services, Meta apps, or Amazon's retail infrastructure are still trackable across those surfaces, with substantially more data than any independent ad network could collect.

- **Authenticated identity infrastructure.** Solutions like UID2 and ATS replace cookie-based cross-site tracking with authentication-based cross-site tracking. From a user privacy perspective, the tracking is still occurring, it is simply anchored to a consent-based authentication event rather than an invisible cookie. If the consent mechanism is dark-patterned or obscured in terms of service, the practical privacy outcome may not be better.
- **Server-side and CNAME workarounds.** CNAME cloaking routes third-party tracking through a DNS alias that makes third-party requests appear as first-party. Server-side tracking collects the same behavioral data but from infrastructure the browser cannot inspect or block. These techniques are available to sophisticated operators and maintain significant tracking capability outside of browser restrictions.

> **Digital 520 Perspective**
>
> The Privacy Sandbox has been criticized by privacy advocates as a Google-controlled transition designed primarily to protect Google's advertising business under the appearance of a privacy improvement. The EFF's Lorrie Faith Cranor and others have noted that Google's advertising data collection within its authenticated user base is entirely unaffected by Privacy Sandbox. The architectural shift does meaningfully constrain independent ad networks while Google's own data position strengthens. Evaluating the privacy implications requires acknowledging this structural dynamic, not just the technical properties of the APIs.

Consent Architecture and Compliance

For organizations operating in GDPR, UK GDPR, or CCPA jurisdictions, cookie deprecation does not reduce the compliance burden: it changes its shape. Consent management remains required for any processing of personal data through tracking, regardless of whether that tracking uses cookies, authenticated IDs, or server-side mechanisms.

Tracking Method	Requires GDPR Consent?	Notes
Third-party cookies (behavioral)	Yes, legitimate interest insufficient per most DPA guidance	CNIL, ICO, and most DPAs have ruled that behavioral advertising cannot rely on legitimate interest lawful basis.
First-party cookies (analytics, session)	Depends on use, session cookies exempt; analytics requires consent	Strictly necessary cookies are exempt. Analytics that build user profiles require consent or anonymization.

Tracking Method	Requires GDPR Consent?	Notes
Privacy Sandbox APIs (Topics, Protected Audience)	Position unclear, evolving regulatory guidance	Topics API processes inferred interests. Several European DPAs are evaluating whether the APIs constitute processing of personal data under GDPR.
Server-side tracking with hashed email	Yes, if linked to identifiable individual	Hashed email is still personal data under GDPR if the hash can be reversed or the individual is otherwise identifiable.
Contextual advertising (no user data)	No consent required	Processing page content to serve relevant ads does not constitute personal data processing if no individual user data is collected or processed.
Authenticated identity (UID2, ATS)	Yes, consent required at point of authentication	Authentication event must include informed disclosure that the identifier will be used for cross-site advertising.

Table 5. GDPR consent requirements by tracking method. Note: Regulatory positions continue to evolve; consult legal counsel for jurisdiction-specific guidance. Source: Digital 520 Analysis.

The Data Minimization Imperative

GDPR's data minimization principle requires that personal data collected must be adequate, relevant, and limited to what is necessary in relation to the purpose for which it is processed. Third-party cookie infrastructure was architecturally opposed to this principle: it was designed to collect as much data as possible, on the theory that more data always has value.

The post-cookie environment creates structural pressure toward data minimization because the mechanisms that enabled promiscuous collection are being technically constrained. This is an opportunity for organizations to rethink their data strategy from first principles: what data do we actually need? What are we doing with what we have? Are we collecting data in ways that users would recognize as proportionate if they were aware of it?

Organizations that approach this as a compliance exercise, finding the minimum technical change required to continue existing data collection practices, will likely face continued regulatory exposure as enforcement evolves. Organizations that approach it as a genuine strategic question about what data is worth collecting and maintaining will build more durable first-party data assets with less legal and reputational risk.

Part V: Practical Guidance by Role

The transition away from third-party cookies requires different actions from different parts of an organization. This section provides role-specific guidance organized around the decisions and technical tasks each function needs to own.

For Engineering and Technical Teams

The following are the priority technical tasks for engineering teams managing the deprecation transition:

- **Audit your cookie inventory.** Use browser DevTools, a privacy scanning tool (OneTrust, Cookiebot, or a custom crawler), or a web application firewall log analysis to enumerate every cookie set on your properties, including first-party, third-party, session, and persistent. Categorize each by purpose: strictly necessary, functional, analytics, or advertising. This audit is the prerequisite for every other step.
- **Classify and remediate SameSite attributes.** Any third-party cookie that needs to function in a cross-site context must carry SameSite=None; Secure. First-party session and authentication cookies should be set to SameSite=Strict or SameSite=Lax. Audit your Set-Cookie headers and fix any that are missing SameSite declarations.
- **Implement server-side Conversion APIs.** For each ad platform you use (Google, Meta, TikTok, LinkedIn, Pinterest), implement the server-side Conversion API as a complement or replacement for client-side pixel tracking. This requires a server endpoint that receives client events, enriches them with server-side data (order ID, hashed email, hashed phone), and forwards them to the platform API. Meta CAPI and Google Ads Conversion API documentation provide implementation guides.
- **Evaluate and implement Google Privacy Sandbox APIs.** For Chrome-targeted campaigns, test Topics API integration by implementing the document.browsingTopics() call in ad decision logic. For retargeting use cases, prototype Protected Audience API integration: joinAdInterestGroup() for advertiser site tagging and runAdAuction() for publisher-side auction logic. Monitor Privacy Sandbox developer documentation for API stability changes.
- **Implement CHIPS for functional third-party embeds.** If your service is embedded in other sites (SSO widget, checkout module, customer service chat), migrate third-party cookies to use the Partitioned attribute (CHIPS). This allows your embed to maintain state within the context of each specific embedding site without enabling cross-site tracking.
- **Audit and update your consent management implementation.** Verify that your CMP correctly enforces consent choices at the tag/pixel level, meaning tracking tags do not fire until consent is granted. Test in Safari and Firefox as well as Chrome. If using Google Consent Mode v2, ensure that the default state for analytics and advertising tags is 'denied' until consent is collected.

⚙ Consent Mode v2 Implementation Note

Google Consent Mode v2 (required as of March 2024 for EEA traffic) sends behavioral modeling signals to Google even when consent is denied, allowing Google to model conversion behavior using aggregate patterns. From a user privacy standpoint, this means that declining consent does not prevent Google from using behavioral patterns from your site for modeling purposes.

From a compliance standpoint, the CMA and several European DPAs have expressed concerns about whether modeling based on non-consented data is compatible with GDPR. If your organization has operations in the EU, consult legal counsel on your Consent Mode v2 implementation before concluding it resolves your consent obligations.

For Marketing and Advertising Teams

The strategic shift for advertising teams is from renting audience data (buying third-party behavioral segments) to owning audience relationships (building first-party data through value exchange). This transition is not primarily technical, it is about reorienting how your organization thinks about user relationships.

- **Audit your current attribution model.** Identify what percentage of your conversion attribution currently depends on third-party cookies. Multi-touch attribution models that rely on cross-site cookie stitching are already broken for Safari and Firefox users, and will degrade further in Chrome. Understand what your current data quality is before assuming your measurement is accurate.
- **Invest in authenticated value exchange.** Email subscription programs, loyalty accounts, preference centers, and gated content are the mechanisms by which users voluntarily provide authenticated identity. The organizations best positioned for the post-cookie environment are those with large authenticated user bases. Treat email and account acquisition as a strategic data asset, not a marketing tactic.
- **Build platform-specific audiences natively.** Within walled gardens (Google, Meta, Amazon), first-party customer match lists uploaded directly are more reliable than behavioral targeting built on third-party data. Customer match on Google and Meta allows you to target known customers, find lookalike audiences, and measure incremental lift against your own customer data.
- **Test contextual campaign structures.** Allocate budget to contextual campaigns on inventory where behavioral targeting was the primary strategy. Measure cost per acquisition difference between contextual and behavioral targeting. Many marketers find the gap smaller than expected for categories with strong content-intent correlation.

For SMBs and Lean Organizations

For organizations without dedicated privacy engineering or legal resources, the path of least resistance and lowest risk is the simplest architecture: use fewer tracking tools, use them transparently, and rely on first-party data and contextual approaches where possible.

Priority	Action	Why It Matters
1 — Immediate	Implement a CMP that blocks all non-essential tracking tags until consent is given	Required for GDPR/CCPA compliance. Protects against regulatory fines. Many platforms (Cookiebot, CookieYes) offer SMB-priced plans.
2 — Near-term	Migrate from Universal Analytics (deprecated) to GA4 with consent mode and IP anonymization enabled	Universal Analytics has been sunset. GA4 with consent mode is the current standard for privacy-compliant analytics.
3 — Near-term	Implement Meta CAPI and Google Conversion API server-side events for your primary ad platforms	Recovers conversion data lost to ITP, iOS ATT, and ad blockers. More stable than client-side pixel tracking.
4 — Medium-term	Build an email list with explicit consent and a clear value proposition	Authenticated first-party audience is the most resilient long-term asset. Not subject to browser or platform changes.
5 — Medium-term	Audit and reduce third-party script load on your site	Each third-party script is a potential source of tracking, security risk, and page performance degradation. Reduce to the minimum needed.

Table 6. Priority action framework for SMBs navigating the post-cookie transition. Source: Digital 520 Analysis.

For Publishers and Media Companies

Publishers face the most direct impact from the cookie transition because their advertising revenue model has historically depended on programmatic ad rates that reflect cookie-based audience targeting. The strategic response requires both technical investment and business model adaptation.

- **Build first-party registration and login.** Authentication is the publisher's most powerful tool in the post-cookie environment. Users who create accounts and log in provide authenticated identifiers that can be used with UID2, ATS, or PPID solutions, and enable deterministic rather than probabilistic audience matching. Even a modest logged-in audience (10-20% of regular readers) significantly improves programmatic CPMs.
- **Implement a subscription or newsletter strategy.** Email as a first-party channel is resilient to all browser and platform changes. Publishers with large email audiences have an authenticated first-party asset that cannot be deprecated. The trend toward reader revenue (subscriptions, membership, newsletters) is not just a business model shift, it is a data strategy.

- **Evaluate direct data partnerships via clean rooms.** Clean room partnerships with advertisers allow publishers to demonstrate campaign effectiveness to advertisers using first-party data match, without exposing individual user records. This positions the publisher as a premium first-party data provider rather than a commodity programmatic impressions source.
- **Pressure-test your programmatic stack for Sandbox readiness.** Work with your SSP to verify Protected Audience API and Topics API integration status. Many SSPs have partial implementation. If your SSP does not have a clear Privacy Sandbox integration roadmap, this is a risk to address.

Conclusion

Third-party cookies were an accident of history: a general-purpose session mechanism repurposed at scale into a cross-site surveillance infrastructure that most users never consented to and many would reject if they understood it. The fact that 75% of iOS users declined ad tracking when asked directly, with a clear prompt, tells you everything you need to know about the gap between technical capability and genuine consent.

The deprecation is real, the timeline is messy, and the replacements are imperfect. Privacy Sandbox APIs provide meaningfully better privacy properties than third-party cookies in some dimensions while introducing new concerns in others. Server-side tracking removes user-visible tracking without necessarily reducing the underlying data collection. Authenticated identity solutions preserve cross-site targeting but anchor it to consent events that vary widely in quality.

The organizations that navigate this transition well will be the ones that treat it as a prompt to build something more durable: data relationships that users understand and choose to participate in, measurement infrastructure that does not depend on tracking invisible to users, and advertising strategies grounded in what users actually tell you rather than what can be inferred from watching where they go.

Key Implications for Your Organization

- Audit your current cookie usage before assuming your tracking infrastructure still works; ITP and Firefox blocking have been degrading data quality for years.
- Server-side Conversion API implementation is the highest near-term ROI technical investment for most advertising-dependent organizations.
- Privacy Sandbox APIs are available but adoption is early. Engineering teams should prototype now, not wait for industry consensus.
- First-party authenticated identity is the only durable long-term alternative. Everything else is a bridge.
- Contextual advertising offers a structurally clean, consent-free approach that outperforms behavioral targeting in high-intent content categories.
- Consent must be real, not a design exercise in coercing acceptance. Regulatory enforcement is closing the gap between dark-pattern consent and genuine choice.

Appendix A: Methodology

Digital 520 applies a rigorous, multi-source research methodology to every Insight Report. For this report on cookie deprecation, the following methods were employed:

- **Primary technical documentation.** Google Privacy Sandbox developer documentation, Apple WebKit ITP technical writeups, W3C specifications for the SameSite cookie attribute, CHIPS, Storage Access API, and Topics API were reviewed in full. All technical characterizations of API behavior are based on official specification documents rather than secondary summaries.
- **Regulatory source review.** GDPR text (Regulation (EU) 2016/679), ePrivacy Directive (2002/58/EC), CCPA/CPRA text, DMA (Regulation (EU) 2022/1925), and enforcement decisions from CNIL, ICO, and the Irish DPC were reviewed. Regulatory guidance on cookie consent lawful basis is drawn from CNIL and ICO published guidance, which are the most specific and widely cited.
- **Academic and industry research.** Research on browser fingerprinting (EFF Panopticlick, Princeton Web Transparency and Accountability Project), cookie syncing mechanics (Englehardt & Narayanan 2016 OpenWPM study), and ATT opt-in rates (Flurry/Yahoo longitudinal tracking) was reviewed and cited. Where industry research reflects vendor interests, findings were corroborated against independent sources.
- **Practitioner judgment.** Digital 520's advisory experience across privacy engineering, advertising technology, and compliance engagements informs the practical guidance in Part V. Implementation recommendations reflect patterns observed across client engagements. Where recommendations reflect practitioner judgment rather than published standards, this is noted.

Limitations: Browser behavior and Privacy Sandbox API specifications are subject to rapid change. Policy positions from regulatory bodies continue to evolve, particularly regarding Privacy Sandbox APIs and Consent Mode v2. All technical specifications should be verified against current documentation before implementation.

Appendix B: Glossary

Term	Definition
ATT (App Tracking Transparency)	Apple's iOS 14.5+ framework that requires apps to explicitly request user permission before accessing the IDFA (Identifier for Advertisers) for cross-app tracking. Opt-in rates settled at approximately 25% globally.
CHIPS (Cookies Having Independent Partitioned State)	A browser mechanism that allows third-party cookies to be partitioned by top-level site, enabling functional embeds (widgets, checkout modules) without enabling cross-site tracking.

Term	Definition
Clean Room	A secure computing environment in which two parties can perform joint data analysis without exposing raw individual-level records to each other. Uses encryption and differential privacy to prevent reconstruction of individual data from aggregate results.
CMP (Consent Management Platform)	Software that presents cookie and tracking consent choices to users, records consent signals, and enforces those signals by blocking tracking tags that have not received appropriate consent.
Contextual Advertising	Advertising targeted based on the content of the page being viewed rather than the behavioral profile of the user viewing it. Requires no personal data processing and no consent under GDPR.
Cookie Syncing	A mechanism by which two ad networks share and link their respective user cookie IDs by passing identifiers through pixel redirect chains, enabling cross-network audience matching and data combination.
Differential Privacy	A mathematical privacy framework that adds calibrated statistical noise to query outputs to prevent the reconstruction of individual-level data from aggregate results. Used in Privacy Sandbox Attribution Reporting API and clean room implementations.
Fingerprinting	A technique for identifying a browser or device based on the combination of technical characteristics (user agent, screen resolution, fonts, canvas rendering, etc.) without using cookies. Highly effective even when cookies are blocked.
GDPR	General Data Protection Regulation (EU) 2016/679. The primary EU privacy law, in force since May 2018. Requires a valid lawful basis (including consent) for processing personal data, including cookie-based identifiers.
IDFA (Identifier for Advertisers)	Apple's device-level advertising identifier, analogous to a third-party cookie for the mobile app environment. Access requires explicit opt-in under ATT on iOS 14.5+.
ITP (Intelligent Tracking Prevention)	Apple's browser-level tracking protection technology in Safari, which uses machine learning to classify tracking domains and restrict or block third-party cookie access and cross-site storage.
Privacy Sandbox	Google's initiative to develop browser-native APIs that provide privacy-preserving alternatives to third-party cookie-based advertising functions (targeting, measurement, attribution) in Chrome.
Protected Audience API	A Privacy Sandbox API (formerly FLEDGE) that enables on-device retargeting auctions without cross-site cookie syncing, by storing interest group membership in the browser and executing bid logic in isolated JavaScript worklets.
RTB (Real-Time Bidding)	The automated auction mechanism in which digital ad impressions are bought and sold in milliseconds, with DSPs bidding based on user behavioral data linked via shared cookie identifiers.

Term	Definition
SameSite Attribute	An HTTP cookie attribute that controls whether cookies are sent on cross-site requests. SameSite=None allows cross-site use (required for third-party cookies); SameSite=Lax and SameSite=Strict restrict cross-site access.
Topics API	A Privacy Sandbox API that provides browsers with interest categories (topics) based on local browsing history for use in interest-based advertising, without exposing individual site visit history to ad networks.
UID2 (Unified ID 2.0)	The Trade Desk's open-source authenticated identity framework that uses hashed email addresses to create a persistent cross-site identifier anchored to user authentication events.

Endnotes

1. Englehardt, S. & Narayanan, A. "Online Tracking: A 1-million-site Measurement and Analysis." Princeton Web Transparency and Accountability Project. ACM CCS 2016. https://webtransparency.cs.princeton.edu
2. Flurry Analytics / Yahoo. "iOS 14.5 Opt-In Rate: Daily Updates Since Launch." April 2021 onwards. https://www.flurry.com
3. Google. "Privacy Sandbox Timeline." developer.chrome.com/docs/privacy-sandbox. Accessed March 2026. https://privacysandbox.com/timeline/
4. International Association of Privacy Professionals (IAPP). "Global Privacy Law and DPA Directory." 2025. https://iapp.org/resources/global-privacy-directory/
5. Kristol, D. & Montulli, L. "RFC 2109: HTTP State Management Mechanism." Internet Engineering Task Force. February 1997. https://www.rfc-editor.org/rfc/rfc2109
6. West, M. & Goodwin, M. "SameSite Cookies Explained." web.dev, Google. https://web.dev/articles/samesite-cookies-explained
7. Interactive Advertising Bureau (IAB). "OpenRTB API Specification." https://www.iab.com/guidelines/real-time-bidding-rtb-project/
8. Englehardt, S. & Narayanan, A. "Online Tracking: A 1-million-site Measurement and Analysis." (cookie syncing section) ACM CCS 2016.
9. Forbrukerradet (Norwegian Consumer Council). "Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us From Exercising Our Rights to Privacy." June 2018. https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf
10. Commission Nationale de l'informatique et des libertés (CNIL). "Cookie consent: CNIL fines GOOGLE €150 million and FACEBOOK €60 million for non-compliance." January 2022. https://www.cnil.fr/en/cookie-consent-cnil-fines-google-150-million-and-facebook-60-million-non-compliance
11. International Association of Privacy Professionals (IAPP). "US State Privacy Legislation Tracker." 2025. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/
12. WebKit Blog. "Intelligent Tracking Prevention." September 2017. https://webkit.org/blog/7675/intelligent-tracking-prevention/
13. StatCounter GlobalStats. "Browser Market Share Worldwide." 2025. https://gs.statcounter.com/browser-market-share
14. Google. "Building a more private web: A path towards making third party cookies obsolete." Chromium Blog. August 2019. https://blog.chromium.org/2019/08/potential-uses-for-privacy-sandbox.html
15. UK Competition and Markets Authority. "Investigation into Google's Privacy Sandbox browser changes." Final Report. 2022. https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-changes
16. Google. "User Choice Rollout Update." Privacy Sandbox documentation. 2024. https://privacysandbox.com/news/
17. Google. "Topics API Developer Guide." developer.chrome.com. https://developers.google.com/privacy-sandbox/relevance/topics
18. Google. "Protected Audience API Developer Guide." developer.chrome.com. https://developers.google.com/privacy-sandbox/relevance/protected-audience
19. Google. "Attribution Reporting API." developer.chrome.com. https://developers.google.com/privacy-sandbox/relevance/attribution-reporting
20. The Trade Desk. "Unified ID 2.0: An Open-Source Standard for the Open Internet." https://www.thetradedesk.com/us/knowledge-center/unified-id-2-0
21. International Association of Privacy Professionals (IAPP). "Data Clean Rooms: Privacy and Advertising Technology." 2023. https://iapp.org
22. Electronic Frontier Foundation. "Browser Fingerprinting: An Introduction and the Challenges Ahead." https://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy