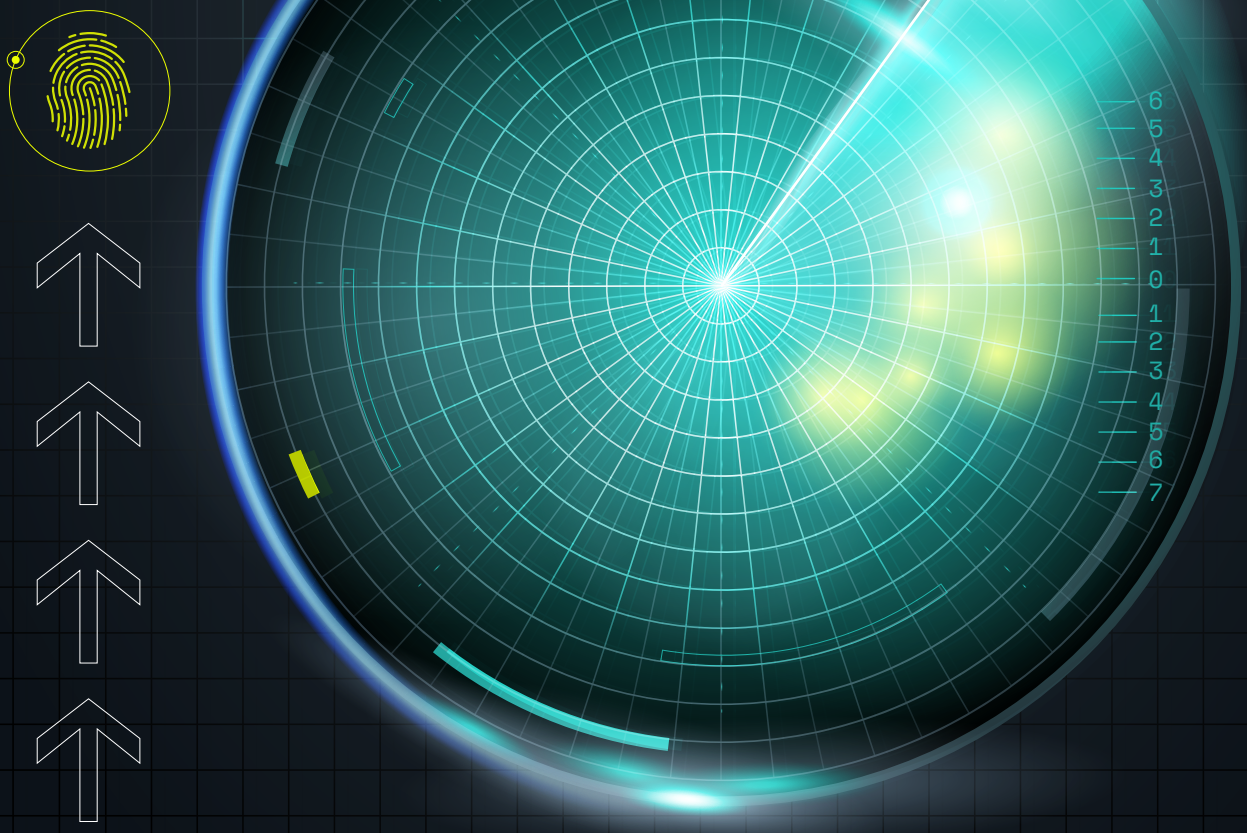
KEPLER

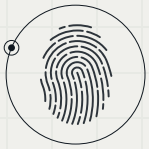
NAVIGATING DIGITAL MEDIA SERIES

Fingerprinting in AdTech

The Future of Tracking in a Privacy-First World



MARCH 2025



With Google's recent policy update, which takes a more relaxed stance on fingerprinting, the conversation around privacy, compliance, and ethical use has become more critical than ever. Kepler's Biddable Product Lead Jonathan D'Souza-Rauto and Associate Account Director Marco Bettini explore how fingerprinting works, its application in AdTech for ad targeting, cross-device tracking, and fraud detection, and why it remains a controversial practice.

As the digital advertising landscape continues to evolve, the methods used to track and identify users have become more sophisticated. One such technique is fingerprinting, a method that aggregates various device and browser signals to create a unique identifier for users — without relying on cookies. Unlike cookies, which users can delete or block, fingerprinting operates server-side, making it a persistent tracking mechanism that raises both opportunities and concerns within the industry.

With Google's recent policy update, which takes a more relaxed stance on fingerprinting, the conversation around privacy, compliance, and ethical use has become more critical than ever.

This report examines the potential regulatory challenges fingerprinting may face, how advertisers, publishers, and vendors can navigate these changes, and what the future of identity tracking looks like in an increasingly privacy-focused world.

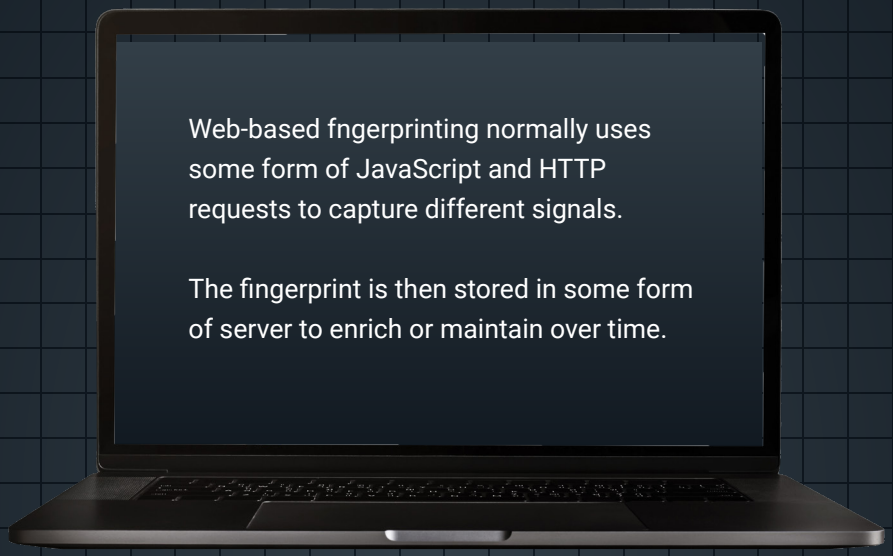
What is fingerprinting?

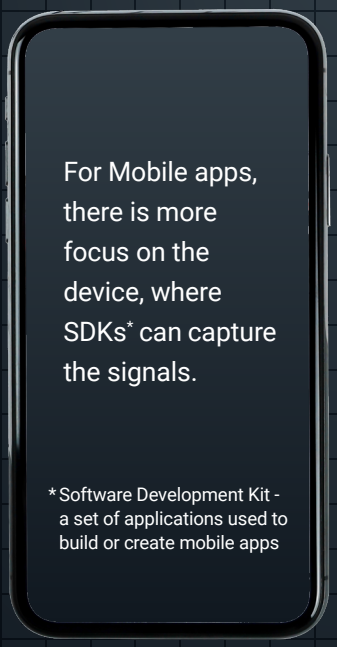
Fingerprinting identifies users across the web by aggregating different signals to construct a unique profile. Unlike cookies, which are stored in the browser and can be deleted by users, Fingerprinting relies on collecting various device and browser characteristics (such as IP address, user agent, screen size, and fonts) and storing them server-side.

This method is used for ad targeting, cross-session and cross-device tracking, and fraud detection. However, it is often considered controversial due to privacy concerns, as users cannot easily consent to or control how their data is collected. Regulatory bodies and major tech companies like Google and Apple have taken measures to limit or regulate fingerprinting in their browsers due to its potential ethical and legal implications.

AdTech fingerprinting is like a passport but in the internet world- less static and ever-evolving.

How does fingerprinting work?





Signal Examples

IP Address
User Agent
Timestamp
Screen Size
Fonts/Themes
Session Cookies
Browser Language

The process of fingerprinting explained

1

Client Side/Browser

HTTP Request

Header Passback

User Agent, Referrer, IP, Address, Language

Server

A request is made from a browser to populate content for a website. A HTTP request is sent to a server for this information, which contains some key characteristics in the header of the request to use for fingerprinting.

2

Server

Header Passback

User Agent, Referrer, IP, Address, Language

Fingerprint #1

A server can then take a combination of the different headers and try to create a fingerprint, which is stored server side. Hashing can be used here to add further persistence alongside security, as well as preparing for some JavaScript functions to run on the client side once pushed back.

3

Server

HTTP Request

Header Passback

User Agent, Referrer, IP, Address, Language

Fingerprint #1

Client Side/Browser

A HTTP Response is sent back to the browser, allowing the website content to populate alongside data in the background, which can include the newly formed fingerprint, stored sometimes in a 1st party cookie.

4

Client Side/Browser

AJAX Request

JavaScript

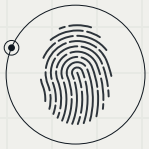
Fingerprint #1

Client Side Data

Fonts/Themes, Timestamp, Screen Size

Server

To enrich the fingerprint, the use of JavaScript can pull data beyond the HTTP request headers in the browser, which is then sent back to the server asynchronously without needing to refresh the page/content.



What are examples of fingerprinting in AdTech?

Analytics tools may infer certain metrics from a fingerprint, particularly cross-device like sessions or key events like a conversion.

Alternative ID solutions can take a probabilistic approach with fingerprinting to build up an ID graph, which works on the idea of stitching together different touchpoints to a known user.

A fingerprint can be used to spot fraudulent/bad actors to aid their removal.

It is quite rare for a vendor or company to admit they are fingerprinting, given its negative connotations and potential legal implications.

Why is fingerprinting considered negative?

Difficult to Police and Regulate

It is nearly impossible to monitor the existence of a fingerprint, determine how it is used, or control who has access to it. This lack of transparency makes it difficult to enforce data protection laws.

Lack of User Consent and Control

Users cannot easily consent to fingerprinting or control how their data is collected, unlike cookies, which they can delete. This raises privacy concerns as individuals are unknowingly tracked.

Privacy and Ethical Concerns

Fingerprinting is a probabilistic method that may use deterministic variables (such as IP addresses), which can lead to excessive tracking and profiling of individuals without their knowledge.

Legal and Regulatory Challenges

Certain characteristics used in fingerprinting, like IP addresses, are considered personal data in UK and Europe. This makes fingerprinting subject to strict regulatory laws, creating compliance risks for businesses using this technique.

Google Ad Policy Update for February 2025

On 18th December 2024, Google announced upcoming policy updates for all its ad platforms, set to take effect on 16th February 2025. These changes primarily impact how advertisers, vendors, and publishers track users across digital channels like Connected TV and Game Consoles.

Notably, Google has adopted a more lenient approach toward fingerprinting — a tracking method that combines various signals and identifiers, such as IP addresses, to link users across browsers and devices. The company attributes this shift to advancements in Privacy Enhancing Technologies (PETs), suggesting that fingerprinting and similar tracking techniques are now more viable and secure than before.

> We think this change is irresponsible. Google itself has previously said that Fingerprinting does not meet users' expectations for privacy, as users cannot easily consent to it as they would cookies. This in turn means they cannot control how their information is collected. To quote Google's own position on Fingerprinting from 2019: "We think this subverts user choice and is wrong."
>
> — Stephen Almond
> ICO EXECUTIVE DIRECTOR OF REGULATORY RISK

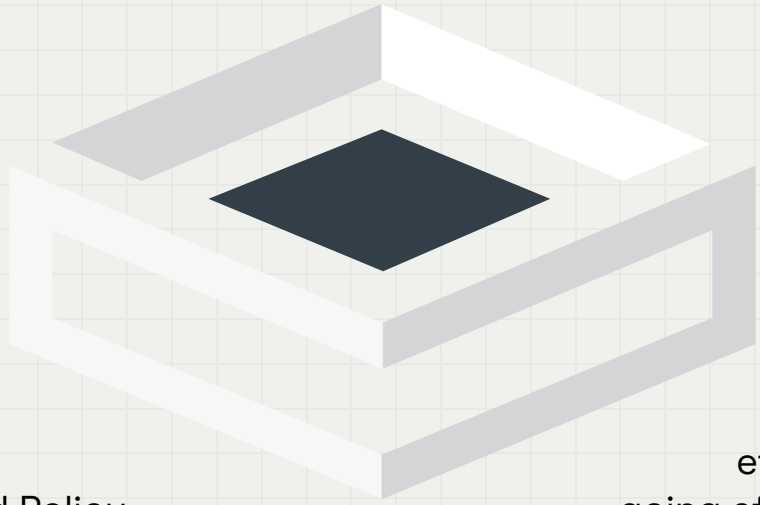
IP Protection Update on the Privacy Sandbox

What Happened?

On 12th February 2025, Google Chrome's Privacy Sandbox team released a list of masked domains (MDL) that will be impacted by their IP Protection proposal, which is scheduled to launch in May 2025.

The IP Protection proposal is aimed at protecting Chrome users' IP addresses as they browse from being used for tracking by third parties. The initial implementation of this is specific to incognito users who also may signed into their Google account on Chrome before starting a session.

To determine whether a site is first party or third party, this builds on a separate Privacy Sandbox proposal called Related Website Sets (RWS), which allows a publisher to determine relationships of their domains/subdomains amongst their portfolio.



Isn't this the opposite of the recent Google Ad Policy change?

The Masked Domains List is actually sourced from a 3rd party called Disconnect.me, which also includes several Google AdTech domains such as ad.doubleclick.net and dartsearch.net, so shows some level of neutrality to potentially appease the regulators.

But there certainly seems to be a different opinion on whether fingerprinting practices are OK from the Chrome side vs Google Ads/Google Marketing Platform (GMP) side. However, the GMP side is predominantly aimed at the CTV market whereas IP Protection is aimed at the web browser.

Is this effectively going after fingerprinting vendors?

Fingerprinting is definitely in the crosshairs of this change, but since the subset of users that are logged into Chrome and are using Incognito mode is not a huge proportion of the overall browser traffic, so its impact is likely to be limited.

This isn't that new to browsers. Apple have used a similar technique on iOS, pulling from DuckDuckGo as the source for their lists. They're employed in a manner similar to versions of Intelligence Tracking Prevention (ITP) which has much stronger restrictions in place compared to Google's approach.

NAVIGATING DIGITAL MEDIA SERIES

What does Google's updates mean for the advertising ecosystem

Impact on advertisers

A short-term but strong solution, likely to face regulatory challenges soon.

Audience data enrichment

Targeting

- Sustain retargeting pools
- Increased focus on first party data

Cross-device tracking

Measurement

- Cross-device and session journey enablement
- Deterministic signals to be offset by probabilistic measurement and data clean rooms

Future eligibility only with consent

Compliance

- Short-term application will be challenged by local regulators
- Tech giants moving away from standard deterministic

Impact on publishers

Dependency on vendors in the future may reduce control over monetisation.

Inventory packaging

Inventory

- Enables premium content segmentation
- Dynamic ad pricing for high-resolution devices

Content and traffic protection

Measurement

- Assess invalid traffic more effectively
- Paywall-protection of non-logged in users

Regulators and tech vendor dependent

Compliance

- Dependency on vendor solutions to future-proof
- Enforcement of consent prior to collection, will be required

Impact on vendors

Utilising data modelling to ensure future-proofing as consent drives walled garden data collection.

Fingerprinting bound by consent

Profiling

- Consent will be paramount even when collection is in aggregate
- Internet service providers to offer new privacy-compliant hybrid signals

Shift to probabilistic solutions

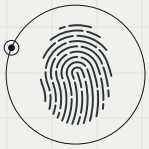
Measurement

- Major browsers to gain more control on the supply chain
- Rise of probabilistic solutions for the rest of the ecosystem

IP address evolution to shape next phase

Compliance

- Use of IP address clashes with privacy regulations, threatening CTV vendors
- Privacy Sandbox measures likely facing additional scrutiny



What is the Future of fingerprinting?

Google Chrome and Android will likely continue to prevent Fingerprinting on its browser/operating system through the Privacy Sandbox.

Apple in a very similar manner have already taken precautions to prevent Fingerprinting on their browser Safari and operating system iOS.

Data regulators will continue to pay close attention to how vendors may leverage this in their products, particularly in relation to consent.

Privacy-enhancing technologies are still a risky bet for linking identities based on probabilities, especially in newer media.

Kepler POV on fingerprinting:

- Fingerprinting remains a contentious practice in the advertising industry, even with Google's evolving stance and advancements in technology.
- The primary concern revolves around privacy, particularly in regions with strict data regulations. When fingerprinting involves personal data, such as IP addresses, it may require implied consent to comply with legal standards.
- Privacy-enhancing technologies can help enable consent before fingerprinting is applied, but they do not fully address the broader challenges associated with this tracking method.
- While fingerprinting can be valuable for fraud detection and bot prevention, it should not be relied upon for identity resolution in paid advertising, as it raises significant ethical and regulatory concerns.

Recommendations for the future

To prepare for the future, advertisers should evaluate alongside partners whether their vendors are using fingerprinting in their services or solutions. If fingerprinting is detected, it is crucial to ask for transparency regarding its implementation, including the signals being collected and the methodology employed. Additionally, staying informed about advancements in Privacy Enhancing Technologies (PETs) is essential, as these innovations may serve as viable alternatives or improvements to fingerprinting. Lastly, organisations must prioritise compliance and risk management by involving legal and security teams to assess regulatory risks and ensure alignment with evolving data privacy laws.