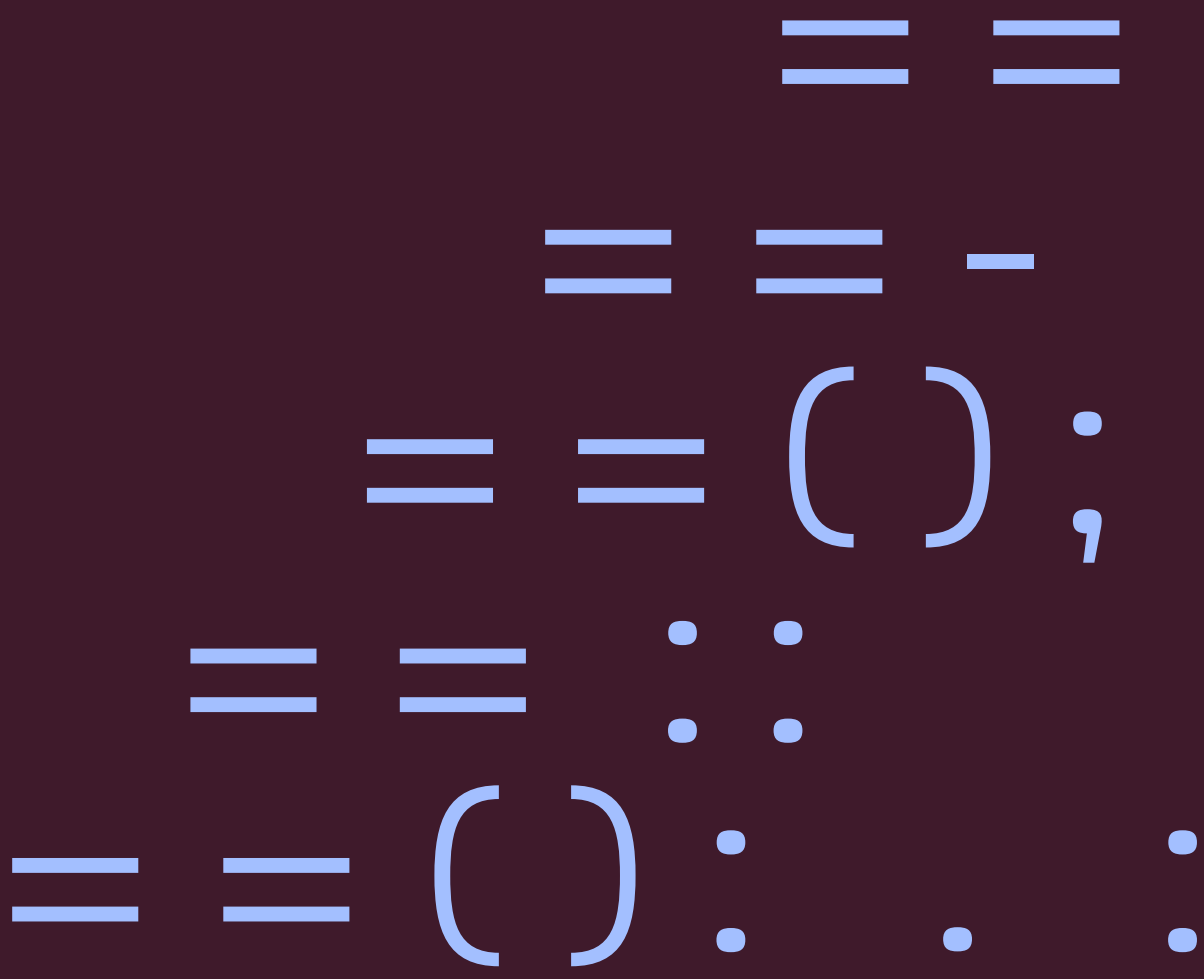
Agency for Digital Government

Handout

Who is Tracking EU Citizens, and How?



December 2024

1. Introduction

This handout accompanies the report *Who is Tracking EU Citizens, and How?* and provides an overview of its key insights. The report aims to shed light on three challenges that arise from third parties collecting data about EU citizens through online services. It does so by analysing 25 popular websites across EU countries. The websites in question represents a diverse field of sectors ranging from social media to e-commerce.

A shift in tracking technologies

This section investigates the increased use of fingerprinting. The analysis finds that all of the websites use fingerprinting, while 50% does it in a manner that is concerning for user privacy.

Managing consent as a business

Consent management platforms (CMPs) are becoming widespread as a means for service providers to achieve compliance. This report finds that 90% of the websites that purchase a CMP solution has at least 1 third party service tracking users before consent.

Online privacy in a globalized world

Global actors drive the prevalent data collection on users. 54 different companies collected data through the analysed websites. 81% of the data that was collected was done so by companies outside the EU.

While this handout presents some of the main findings, the report itself provides further context and implications. Furthermore, please refer to the report for the list of websites that was analysed and the methods applied to do so.

2. A shift in tracking methods

A tracking technology increasingly used for identifying and targeting users, is *browser fingerprinting*. Fingerprinting works through the collection of various data points about the users' device or browser and combines these into a unique 'fingerprint' used to track a user across websites.

Figure 1 shows the results from the analysis. The websites are ranked according to how many individual fingerprinting categories each site collects data from. The individual categories represent a range of different types of data points. An example could be a category called 'Storage' that covers data points such as cookies, local storage, session storage, etc. Based on how many unique categories the websites collect from, they have been divided into whether the likelihood of profiling/tracking taking place is low or medium-high.

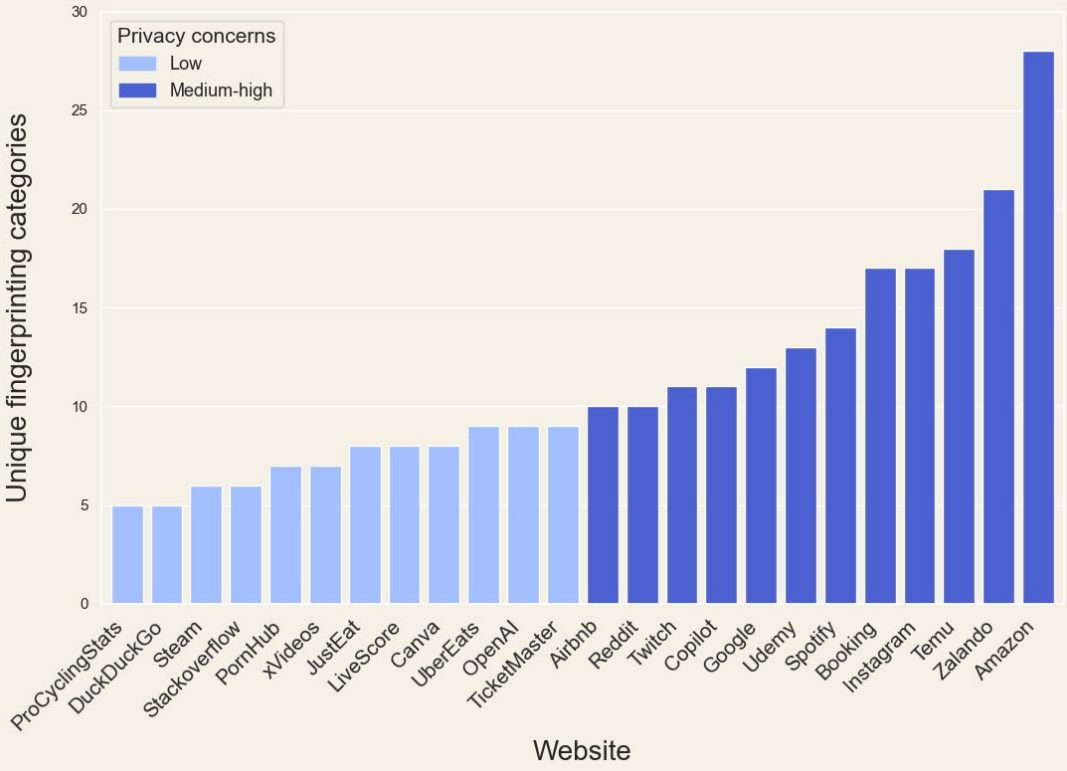


Figure 1: Unique fingerprinting categories across websites.

Fingerprinting can be a highly precise method for tracking users across services. This precision is achieved in a way that is invisible to users and difficult for them to prevent. Through fingerprinting, even ordinary settings like preferred language or browser of choice can make the user easier to identify.

50% of the websites used browser fingerprinting in a manner that is concerning to privacy, and without the user's consent.

3. Managing consent as a business

In the face of regulatory frameworks that introduce limitations on data gathered about users without their consent, service providers have increasingly embraced consent management platforms (CMPs). CMPs are tools that help websites collect, manage, and store user consent for data collection and usage, with the intention of ensuring compliance with privacy regulations. The global market size for CMPs reached $874 million in 2023[1], making it a significant actor in the business of compliance.

90% of the websites using a CMP provider had at least one third-party service tracking the user before consent.

43% of the websites with their own consent solution had at least one third-party service tracking the user before consent.

The analysis of the 25 websites revealed, that 14 used their own solution while 10 used a third party CMP provider. More websites employing a third party CMP had at least one third party tracker activated before user consent than those using their own. These third party services are separate from the CMP providers, meaning the collected data are not used for the management of consent.

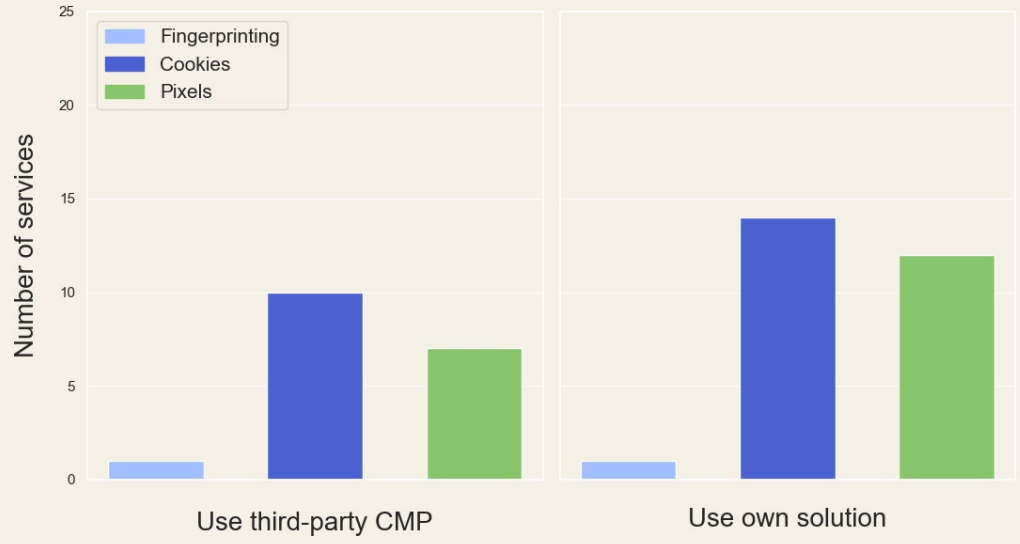


Figure 2: Number of services that mention different tracking technologies in their privacy

Additionally, a part of the service that CMPs offer is generating cookie policies – a requirement for websites that use tracking technologies. Assessing these policies for the websites using a third party CMP reveal that only 1 mention fingerprinting, 7 mention pixels while all mention cookies. (Figure 2)

While it makes sense from a cost perspective, that website owners purchase solutions to manage consent instead of developing their own, it is not immediately clear that these solutions help website owners become compliant. Meanwhile, the responsibility for achieving compliance rests solely on the website owner.

[1] https://www.persistencemarketresearch.com/market-research/consent-management-market.asp

4. Online privacy in a globalized world

Today, global actors shape the digital landscape that we traverse, often by gathering data about users as they use apps and visit websites. This makes much of the data collection on users a cross-border issue, where users from one country have data sent to servers in another country.

54 different companies were tracking users across 25 websites.

Of all the data collected in the present report, 81% was by companies based outside the EU. Previous reports, published by the Danish Agency for Digital Government revealed that companies based in the US is dominant on both websites[2] and in apps[3]. A difference between the two mediums is that data collectors from China are remarkably prevalent in apps, at least on apps for iOS.

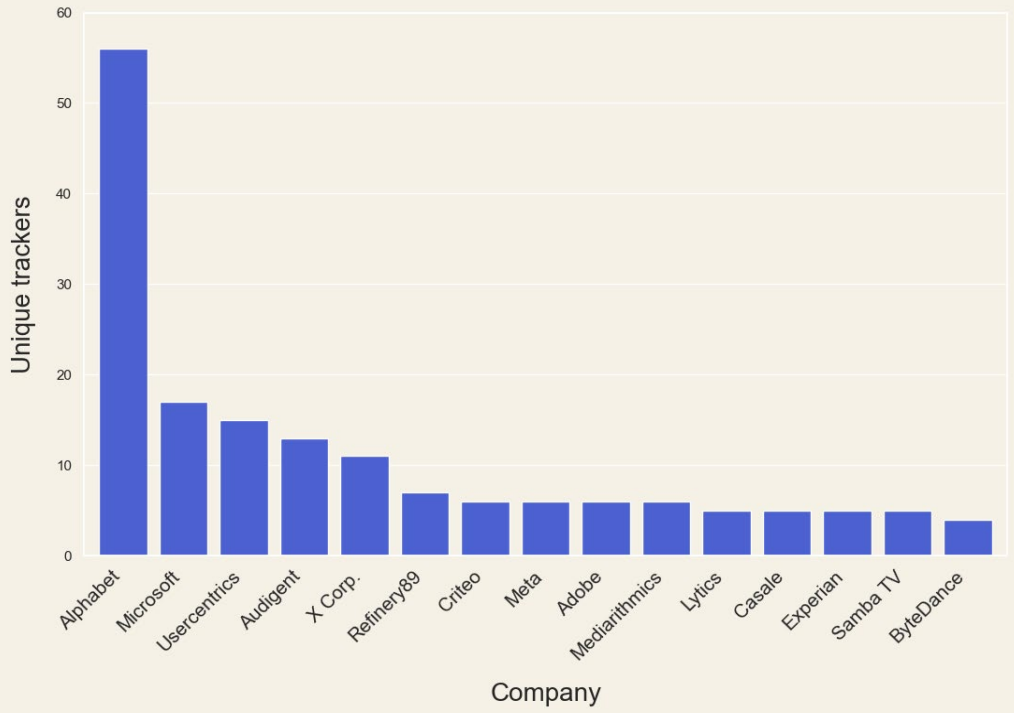


Figure 3: Number of unique trackers per parent company (top 15).

While jurisdictions like the EU have legal frameworks to protect user's privacy, cross-border data collection by big tech companies may give rise to difficulties for consumers' ability to preserve their privacy or know who has data on them.

[2] https://digst.dk/media/31243/what-is-the-cost-of-a-free-mobile-game.pdf
[3] https://digst.dk/media/31245/the-prevalence-of-third-party-services-on-danish-websites.pdf

Agency for Digital Government