Future of online advertising

Adtech's new clothes might redefine privacy more than they reform profiling

As the era of cookie tracking is about to end, a new battle for control over the billion dollar ad tech business has begun. An astonishing partnership between non-profit Mozilla and surveillance capitalist Meta is only a small chapter of a bigger story, argues Michael Veale. For the next phase of online advertising could be even worse.

25.02.2022 um 17:26 Uhr - Gastbeitrag, Michael Veale - in Datenschutz - keine Ergänzungen

Once again, advertising technology is changing. But is the new direction the right one? – Gemeinfrei-ähnlich freigegeben durch unsplash.com Joe Yates

Michael Veale is Associate Professor in digital rights and regulation at University

College London's Faculty of Laws. His research focusses on how to understand and address challenges of power and justice that digital technologies and their users create and exacerbate, in areas such as privacy-enhancing technologies and machine learning. A German translation of the article can be found here.

Mozilla raised eyebrows earlier this month when it announced a collaboration around next-generation advertising technologies with Meta. After all, Firefox's developers once even went so far to create and maintain a "Facebook Container" feature to quarantine this *one specific firm's* cookies.

It's no secret the browser needs to secure funding as its market share dwindles, and it is likely on the look out for powerful friends. But Mozilla's reputation is however only a minor subplot which helps illustrate a much bigger story: a story about the future of what online privacy even *means*.

Apple and Google take control

The Mozilla–Meta proposal concerns *ad attribution*, the art of connecting a user's ad view or click to a later purchase, perhaps even on another device. Classically, this relies upon hundreds of adtech firms' cookies and trackers opportunistically hoovering up individuals' web browsing or app usage history to match views and clicks to actual shopping. In a decision in early February, EU regulators indicated deep, perhaps impossible, change is needed for such tracking practices to be legal in Europe.

Simultaneously, adtech has struggled to adapt as browsers — Chrome and Safari being the most important — increasingly block tracking techniques. Apple, followed soon by Google, are also starting to limit the tracking in apps on iOS and Android, to mixed effect.

But blocking isn't all Apple and Google have done. Crucially, with their power over both the most used web browsers and mobile operating systems they decide what, if anything, fills the vacuum they leave behind. Both firms have, like Meta and Mozilla, designed replacements to existing ad attribution. These replacements promise to end relying on copies of users' intimate browsing histories floating around the adtech ecosystem, instead keeping the data within devices and using it there.

Apple and Google don't spare with privacy rhetoric around their initiatives, but

conveniently these steps to reform adtech would install them as gatekeepers to insights about online users. The two companies would keep the data within browser and operating system infrastructure they entirely control. Google's "Privacy Sandbox" is the highest profile plan in this space — a growing set of tools to move adtech's centre of gravity from between websites, apps and third-party servers to between websites, apps, *browsers* and *operating systems*.

Meta is spooked. It has websites, apps and third party servers in abundance. Browsers or operating systems? None. This leaves the huge adtech firm vulnerable. Apple's recent hiding of app device identifiers allegedly cost Meta $10bn. Its "metaverse" is designed to plant new, deeper infrastructural roots, but the relevant technologies, societal appetite, and even fringe economic importance seem far from inevitable, and a long way off even if they do materialise.

Enhancing privacy and competion?

It is in this context that the Meta–Mozilla ad attribution proposal tries to fight this shift. „Interoperable Private Attribution" tries to match ad interactions and purchases confidentially on big third-party servers using fancy cryptography, rather than keeping the data in the domain of devices and firms that control them.

In essence, it lets apps and websites write, but not read, identifiers on individuals' devices that are associated with particular tracking providers, such as Google or Facebook. These identifiers can be the same across all users devices, if they ever log into these providers on each device. Their devices then encrypt data about adverts they have seen, and money they have spent, and send it alongside the identifier key to two different servers at once. Users must trust these servers not to share data. Working together, these servers alter the data slightly, and send it onwards to the rest of the adtech providers in a form intended to reveal little to nothing about individuals in the dataset, but allow the batched activities of groups of people to be analysed in aggregate.

The Mozilla–Meta proposal particularly plays to a recent saga of competition-versus-privacy, claiming to find a sweet spot amidst concerns of and complaints to competition regulators around the power on-device analysis gives Google and Apple.

It imagines that any firm can set an identifier and provide ad attribution services, not just the device manufacturers — although it requires users to trust these

providers to do the fancy cryptography they are supposed to, and not be tempted to snoop. It also still relies on the browsers and operating systems to buy into this, and play along.

Firms wouldn't see your browsing history, but can still use it

Yet the competition-versus-privacy framing has a gaping flaw. All these moves to shift adtech to know less about individual users, regardless of whether they are mainly on-device or off-device, rely on selecting a very specific, limited definition of privacy to design around. In a way, these ad attribution battles are just the start of *all* functions of adtech, including detailed profiling, shifting to work so that big platforms cannot easily identify their users.

Yet the *confidentiality*, or non-identifiability, of a system should not be equated with the *privacy* it affords. Many, if not most, of the societal issues stemming from profiling, targeting and the commodification of attention are not solved by simply replicating existing adtech while mathematically blindfolding firms to the humans and communities subject to them. There are harms associated with shaping an individual's informational world, learning about specific groups or communities or phenomena, targeting people at opportune moments when they are most suggestible.

These harms do not go away by ensuring firms cannot s*ee* a user's browsing history, but only *use* it. Even if the largely illegal, free-for-all world of adtech data sharing might be on the way out, the scene is being set for a concerning continuation — or even expansion — of profiling, hyperpersonalisation and commodified attention.

Indeed, current proposals for confidential profiling and targeting, such as Google's "Topics" or Meta's "Ad Topic Hints" make only limited use of the wide future possibilities for intense, cryptographically-fuelled, on-device personalisation. Firms from Microsoft to Google are chasing ways to migrate more advanced forms of machine learning modelling into confidential adtech. The specific Meta–Mozilla proposal prides itself on the potential its structure has to extend to machine learning.

It is worth considering that if confidentiality is the main only concern, profiling and modelling could even become *more* invasive than before. Imagine being profiled on your eye gaze, temperature or pulse, with these affecting your online experiences in real-time. But don't panic! It's confidential. What's your problem?

Platforms can't stop discrimination they can't see

This might be mitigated if users could choose whether or not their devices helped profile them or not; an option they never really had when mysterious servers ran the show. But considering past and current trends, it seems unlikely they'll get a meaningful choice. Individuals already lack control over the inscrutable, changing code running silently on their devices.

Even if they *could* switch off profiling, they should expect to be punished for it. Technologies also exist for confidentially *proving characteristics* about users — such, perhaps, as whether their device has profiled and targeted its user enough to warrant an economic reward. Related approaches are already making their way into Google's Privacy Sandbox as anonymous "Trust Tokens" to prove ad viewers are real people, not fraudulent bots. If users aren't obediently running "privacy-preserving" profiling and advertising code, they should eventually expect to be denied their favourite online services.

If this wasn't dismal enough, these practices can give platforms more ways to hide from responsibility. It's already hard enough to hold shady data brokers to account. It may be harder still to hold adtech to account when profiling is siloed cryptographically or kept on device. Conveniently, this blindfolds firms to the potentially discriminatory, fraudulent or democratically hazardous ways these technologies can be abused.

Time to regulate profiling and personalisation

There are better ways to react to these winds of change now than we currently are doing. We should certainly and promptly fix the illegal data leakage that characterises contemporary adtech. Yet we should be careful what we replace it with.

Civil society, regulators, and legislators must stop thinking in terms of mountains of data, where power comes from the ability to accumulate it, and is diminished by letting others have copies of it or reducing its collection. The smart money is on the power firms can gain through *controlling code and computation*, even when data never leaves a device in an identifiable way.

The harms of hoarding data are real, but also old news. Now, the focus needs to move to legal limits to the practices and outcomes from personalisation, profiling, and controlling attention, not just limits to the data shared in the process.

Du möchtest mehr kritische Berichterstattung?

Unsere Arbeit bei netzpolitik.org wird fast ausschließlich durch freiwillige Spenden unserer Leserinnen und Leser finanziert. Das ermöglicht uns mit einer Redaktion von derzeit 17 Menschen viele wichtige Themen und Debatten einer digitalen Gesellschaft journalistisch zu bearbeiten. Mit Deiner Unterstützung können wir noch mehr aufklären, viel öfter investigativ recherchieren, mehr Hintergründe liefern - und noch stärker digitale Grundrechte verteidigen!

Unterstütze auch Du unsere Arbeit jetzt mit deiner **Spende.**

Über den Autor/ die Autorin

Gastbeitrag

Gastbeiträge sind Beiträge von Personen, die nicht zur netzpolitik.org-Redaktion gehören. Manchmal treten wir an Autor:innen und Verlage heran, um sie nach Gastbeiträgen zu fragen, manchmal treten die Autor:innen an uns heran. Gastbeiträge geben nicht unbedingt die Meinung der Redaktion wieder.

Veröffentlicht

25.02.2022 um 17:26

Kategorie

Datenschutz

Schlagworte

Apple, Browser, datenhandel, Edge Computing, english, Facebook, firefox, FLoC, Google, Interoperable Private Attribution, Meta, Michael Veale, Microtargeting, mozilla, Online-Werbung, personalisierte werbung, Privacy Sandbox Initiative, Profiling, Targeted Advertising, Überwachungskapitalismus

0 Ergänzungen

Mit freundlicher Unterstützung von

PALASTHOTEL