The Privacy Sandbox Has Always Been a Farce

By deciding to keep third-party cookies in Chrome, Google delivered the latest punchline in its years-long comedy of errors. And no one is laughing.

As the chief technology officer of an adtech measurement company, I've spent years in the trenches of W3C meetings about the Privacy Sandbox, poring over documents and even submitting an API proposal. Throughout, I've witnessed a masterclass in corporate hubris.

But why exactly couldn't the world's fourth most valuable company get this right?



The monopoly elephant

First, why did Google even bother with the Privacy Sandbox at all? They said they wanted to make "the web more private and

secure for users.” In reality, Google was spurred into action by its paradoxical position as both a dominant monopolist in digital advertising and also a laggard in the even bigger race against Apple to be the true heart of consumers’ digital lives (and thus privy to the minute personal details that will power AI agents.)

Google makes money from search, but people only search when there’s something to find—Google needs a healthy, searchable open web. Web publishers need advertising to make money, and effective advertising requires data. Seeing weakness, Apple seized the marketing moral high ground by loudly attacking Google on privacy.

Google needed a way to simultaneously fend off Apple, protect the searchable web and preserve its panoptic view of a billion-plus users across YouTube, Google Search, Gmail and Android.

The flawed foundation

And so Google appointed itself the arbiter of web privacy standards, unilaterally declared that “privacy” means “preventing cross-site tracking,” and tried to repeat its long tradition of forcing the entire digital advertising industry to play by its rules.

The core problem was that Google’s definition of privacy was philosophically bankrupt. It ignores key common-sense aspects of privacy, such as the notion that users’ expectations vary depending on what information they’re sharing and with whom (i.e. philosopher Helen Nissenbaum’s concept of contextual integrity). Or that harm comes from how data is used, not how it’s collected.

But this rigid, self-serving “cross-site” definition allowed Google to conveniently sidestep any nuanced discussion about data collection, use or sharing that might impact its core

business.

The hypocrisy was obvious in one of the earliest Sandbox proposals: “Related Website Sets,” which allows cross-site tracking for sites owned by a single company (read: Google). In other words, “it’s only a privacy violation when other people do it.”

This impoverished, binary definition of privacy led directly to the series of convoluted Sandbox proposals that were never adequate in either capability or performance. Topics and the Protected Audiences API were doomed from the start, burdened with the impossible mission of supporting usefully targeted advertising while allowing zero cross-site tracking.

Unintended consequences

Google’s absolutist stance has driven many in the industry toward potentially even less privacy-friendly alternatives, like identifiers based on nonresettable personal identifiers such as physical addresses or phone numbers. It also created a climate of hopelessness for the web that accelerated the flow of ad dollars into a monoculture of gigantic walled gardens (like YouTube) that may collect and exploit even more comprehensive user data.

Now, four years in, Google has produced little except unusable, unfixable APIs and a track record of monopolistic bullying that has made Google the target of multiple antitrust prosecutions in the U.S. and a showstopping intervention from the U.K.’s Competition and Markets Authority.

And I will personally try not to think too much about the thousands of hours wasted by those of us gullible enough to believe Google would at least eventually follow through on its stated plans.

The way forward

It is now clear that the Emperor of the Web has no clothes. Google has essentially admitted that the Privacy Sandbox's flaws run too deep to salvage.

To be clear: The public-facing Privacy Sandbox work has been conducted by smart, well-intentioned individuals whom I like and respect. This outcome isn't their fault—the blame lies squarely with Google's executive leadership, who (whether cynically or naively) ordered an impossible mission. But now, because of them, everybody loses.

It should be clear to all that the Wild West era of third-party cookies (and the too often abusive data-sharing they enable) must come to an end. But now, instead, it will limp onward in undeath. Google will retreat into its castle, and nothing will improve for consumers.

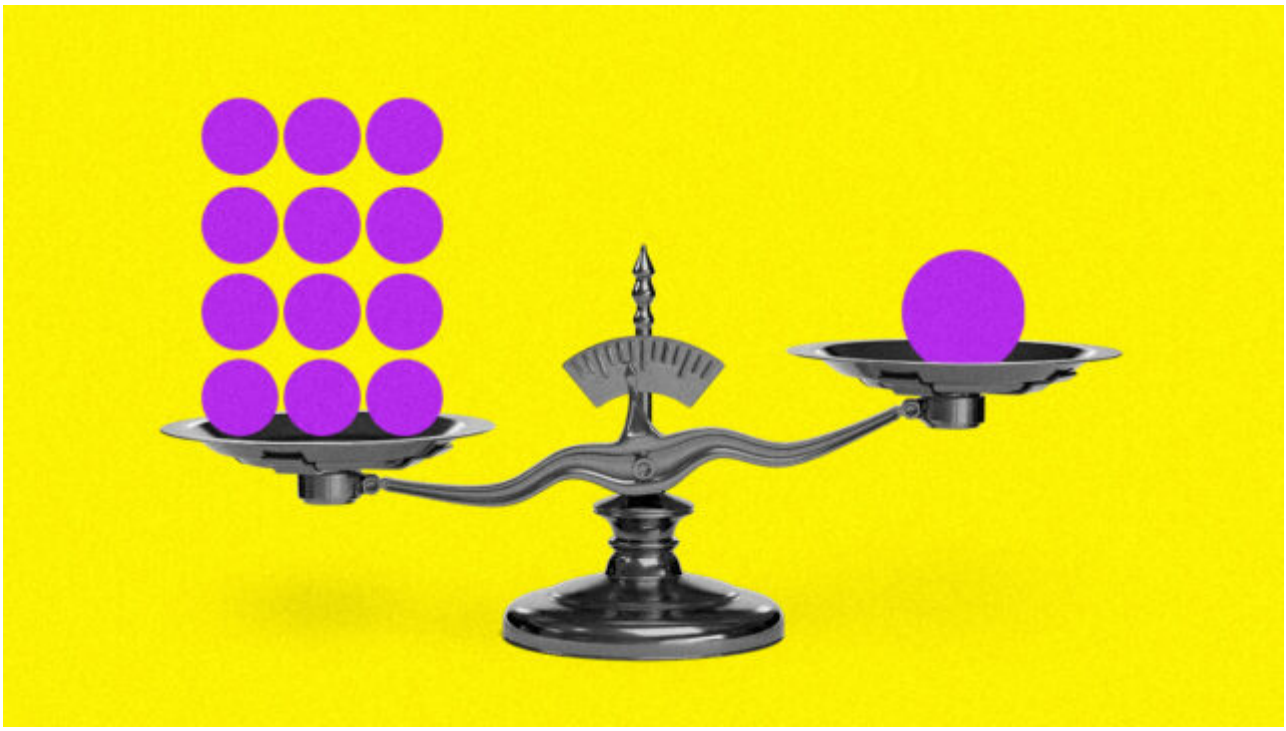
Privacy is a hard problem but not an insolvable one—it boils down to treating users with care and respect. It's time to collectively concede that self-regulation can't and won't succeed, and the only way forward is a true multistakeholder initiative led by regulators with binding authority over gatekeeper web platforms.

The initiative must, at a minimum:

1. Embrace holistic privacy, starting with a comprehensive consensus-building process to understand users' diverse privacy expectations and the complex realities of data (mis)use in the modern web ecosystem.
2. Adopt (and justify) a flexible, dynamic definition of privacy based on philosophical norms and threat modeling of real user harms (including those perpetrated by "first parties" like Google itself).
3. Be ready and empowered to adjudicate conflicting interests, and create enforceable and pragmatic data use

rules.

4. Acknowledge real-world trade-offs between privacy, functionality and competitive market structure.
5. Focus on incremental progress rather than utopian reinvention of the entire digital world.



It’s time to move beyond simplistic privacy dogmatism. It’s time to embrace and nurture the complex, chaotic beauty of the modern internet. And it’s time to develop an international privacy regime that serves and respects users while allowing for innovation and sustainable, “don’t be evil” business models.

This won’t be cheap, easy or fun. But it’s the only way to build a truly privacy-respecting web that works for everyone, not just trillion-dollar giants.

Recommended articles
https://www.adweek.com/programmatic/the-privacy-sandbox-has-always-been-a-farce/