Will Google Play Fair in the ‘Privacy Sandbox?’

On August 22, Justin Schuh, a director on Google’s Chrome Engineering team, introduced the company’s plans for a “privacy sandbox,” a colorful title for its initiative that purports to strengthen web privacy. The news appeared on Google’s blog in an article titled “Building a more private web.”

According to Schuh, the need for a privacy sandbox stems from certain data practices that “don’t match up to user expectations for privacy.” He suggests that when other browsers allow the blocking of cookies, it actually undermines privacy “by encouraging opaque techniques such as fingerprinting.” The fingerprinting technique consists of developers harvesting small bits of data that are unique to users and that collectively can generate a unique identifier that’s available across sites. Schuh claims that Google Chrome wishes to prevent such

a practice: “Unlike cookies, users cannot clear their fingerprint, and therefore cannot control how their information is collected. We think this subverts user choice and is wrong.”

In his August 26 article on ArsTechnica.com, Timothy B. Lee helps demystify the concept of a privacy sandbox for the rest of us: “Under this approach, the browser would impose a hard cap on the amount of information any site could request from the browser that might reveal a user's identity. If a site exceeded the cap, the browser would either throw an error or it would return deliberately inaccurate or generic information.”

Google’s Schuh also claims the blocking of cookies has a steep effect on income for publishers; he says that when ads are made less relevant, such revenues decrease by an average of 52%.

In addition to taking steps to block fingerprinting, Google is developing open standards that purport to “advance privacy, while continuing to support free access to content.” The development of these standards is ongoing and open to comment; a separate article in the Chromium blog includes a summation of the steps.

In the ArsTechnica piece (“Google defends tracking cookies – some experts aren’t buying it”), author Lee suggests browser privacy “has emerged as an important differentiator for Google’s rivals in the browser market.” For example, in the article he notes that Apple has for years provided measures to prevent tracking cookies, Mozilla’s Firefox will soon block such cookies “by default,” and Microsoft is taking steps to place similar protections in the Edge browser.

The nub of the skepticism can be traced directly to revenues, of course. Lee writes: “But Google has a problem: it makes most of its money selling ads. Adopting the same aggressive cookie blocking techniques as its rivals could prevent Google's customers from targeting ads—potentially hurting Google's bottom line.”

A rather blunt criticism of this privacy-sandbox initiative is found on a Princeton University blog called Freedom To Tinker, in a piece titled “Deconstructing Google’s excuses on tracking protection” (August 28). Authors Jonathan Mayer and Arvind Narayanan spare no words in their opening salvo: “Blocking cookies is bad for privacy. That’s the new disingenuous argument from Google, trying to justify why Chrome is so far behind Safari and Firefox in offering privacy protections.”

The writers go on to carefully spell out their skepticism, saying that the blocking of cookies does not undermine privacy; that no solid evidence shows that tracking-based ads are more effective; that Google doesn’t know how to balance privacy demands with ad revenue demands; and that, ultimately, Google is simply stalling – “attempting a punt to the web standardization process, which will at best result in years of delay.”