

How private is your browser's Private mode? Research into porn suggests "not very"

Thought using Incognito mode might keep such searching private? Facebook, Google, and even Oracle have more of your Web usage in their sights than you might think.

reader comments

66 with 54 posters participating, including story author

Share this story

A forthcoming research paper [PDF] from researchers at Microsoft, Carnegie Mellon, and the University of Pennsylvania brings up the possibility that Google and Facebook might be tracking your porn history—and, perhaps more worrisome, that using Incognito mode doesn't help.

The paper, set to be published in the journal *New Media & Society*, does an excellent job of backing up the claim that porn usage ends up being tracked by Google and Facebook. Authors Elena Maris, Timothy Libert, and Jennifer Henrichsen used open source tool webxray to analyze more than 22,000 porn sites, discovering tracking code for Google on 74% and for Facebook on 10% of the sites analyzed. Software giant Oracle's Web tracking code also showed up, appearing on 24% of those sites.

In light of the study, a Facebook spokesperson told CNET, "We don't want adult websites using our business tools since that type of content is a violation of our Community Standards. When we learn that these types of sites or apps use our tools,

we enforce against them.” Google told The New York Times that the company disallows ads on adult sites and directly prohibits adding information based on sexual interest or activities to any personalized advertising profiles.

Oracle is another story entirely. It may come as a surprise to some that the database giant is in the ad-tracking business at all. Oracle has an advertising services division called DataCloud, into which it has funneled more than \$3 billion dollars in acquisitions in the last five years. Oracle Data Cloud’s privacy policy states that “interest segments” are not created for “interest in adult products or services,” but it doesn’t specifically state that such information won’t end up in consumer profiles. Non-profit Privacy International has filed a GDPR complaint against Oracle, alleging that it abuses the “legitimate interest” defense as a cover for collecting information the GDPR and other privacy legislation prohibit.

The ability of Incognito/Private/InPrivate mode in various browsers to defang such tracking is another larger question. The researchers claim that “incognito mode only ensures [one’s] browsing history is not stored on [one’s own] computer,” but the reality is more complex. While the sites you visit do still track Incognito browsing, for the most part this is the difference between tracking “Firstname M. Lastname, see attachments for employment, relationship, hobby and shopping history” and tracking “somebody in a grey hoodie.”

The sites you browse to in Incognito mode do still set and read tracking cookies, but those cookies are not directly connected to the long-lived cookies from your normal browsing sessions. This means that the data brokers are effectively building a brand-new profile based on your Incognito session, and unless you specifically log in to Facebook or Google *inside* that Incognito session, it’s fairly unlikely for the two to become directly connected. IP address tracking is a possibility, but it’s usually too iffy for advertising

use—it's too likely to produce "bleed" from one profile to the next due to things like dynamic IP addresses changing or multiple users in the same household (or, worse yet, business or college campus).

This leaves browser fingerprinting as a method to tie your profiles together—and unfortunately, Incognito mode doesn't appear to help. When we checked the EFF's Panoptick privacy test in both normal and Incognito browsing modes, we saw effectively no difference. If you like to download and install a lot of fonts—or if you install a lot of applications that install their own fonts—you may make yourself highly identifiable, since your browser will report a list of available fonts to any site that requests it. For most people, however, the biggest "smoking gun" techniques for fingerprinting are likely to be the canvas and WebGL fingerprints.

In our testing, even two computers with the same operating system version and screen resolution produced consistent, unique canvas and WebGL fingerprints, which were unaffected by Incognito mode or even by Firefox's hidden `privacy.resistFingerprinting` setting. The most common privacy plugins, such as the EFF's Privacy Badger, didn't help either. The best answer seemed to be the installation of an extension like Canvas Blocker for Firefox or Canvas Blocker (Fingerprint protect) for Chrome, either of which will inject a little random noise into such attempts. This type of precautionary move changed the signature for both fingerprints in the Panoptick test with every visit. Of course, now you're trusting whoever made the extension not to track you—particularly if the extension itself is not open source. As always when it comes to browsing the Internet, the best solution is the simplest: tread carefully.

<https://arstechnica.com/?p=1539027>