WASHPO: Google Chrome has become surveillance software. It’s time to switch.

Our latest privacy experiment found Chrome ushered more than 11,000 tracker cookies into our browser — in a single week. Here’s why Firefox is better.

-
-
-
-

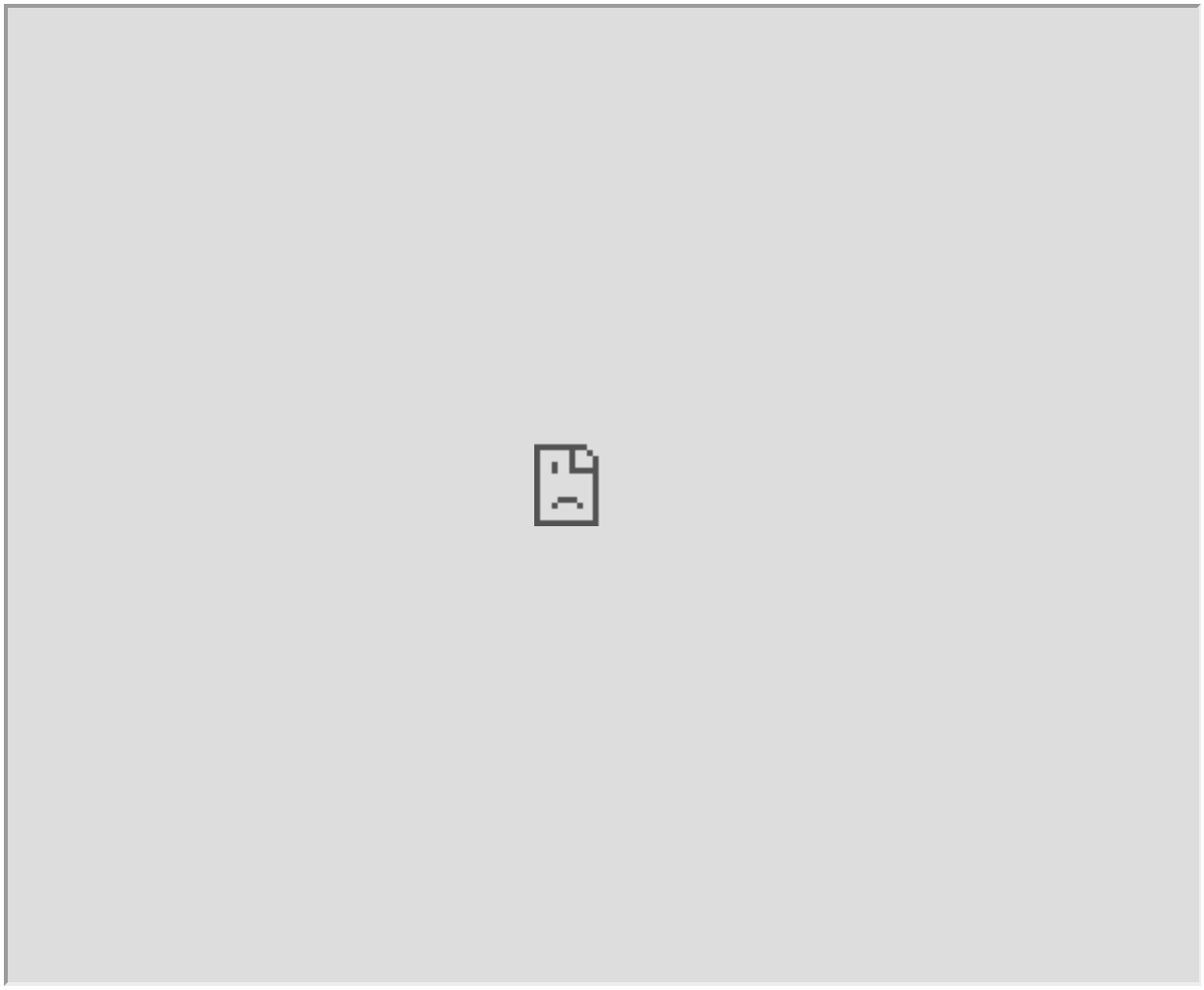
By Washington Post | wapo@dfmdev.com |

By Geoffrey A. Fowler | The Washington Post Columnist

You open your browser to look at the web. Do you know who is looking back at you?

Over a recent week of web surfing, I peered under the hood of Google Chrome and found it brought along a few thousand friends. Shopping, news and even government sites quietly tagged my browser to let ad and data companies ride shotgun while I clicked around the web.

This was made possible by the web's biggest snoop of all: Google. Seen from the inside, its Chrome browser looks a lot like surveillance software.



Lately I've been investigating the secret life of my data, running experiments to see what technology really is up to under the cover of privacy policies that nobody reads. It turns out, having the world's biggest advertising company make the most-popular web browser was about as smart as letting kids run a candy shop.

It made me decide to ditch Chrome for a new version of nonprofit Mozilla's Firefox, which has default privacy protections. Switching involved less inconvenience than you might imagine.

My tests of Chrome versus Firefox unearthed a personal data caper of absurd proportions. In a week of web surfing on my desktop, I discovered 11,189 requests for tracker "cookies" that Chrome would have ushered right onto my computer, but were automatically blocked by Firefox. These little files are the hooks that data firms, including Google itself, use to follow what websites you visit so they can build profiles of your interests, income and personality.

Chrome welcomed trackers even at websites you'd think would be private. I watched Aetna and the Federal Student Aid website set cookies for Facebook and Google. They surreptitiously told the data giants every time I pulled up the insurance and loan service's log-in pages.

And that's not the half of it.

Look in the upper right corner of your Chrome browser. See a picture or a name in the circle? If so, you're logged in to the browser, and Google might be tapping into your web activity to target ads. Don't recall signing in? I didn't, either. Chrome recently started doing that automatically when you use Gmail.

Chrome is even sneakier on your phone. If you use Android, Chrome sends Google your location every time you conduct a search. (If you turn off location sharing it still sends your coordinates out, just with less accuracy.)

Firefox isn't perfect – it still defaults searches to Google and permits some other tracking. But it doesn't share browsing data with Mozilla, which isn't in the data-collection business.

At a minimum, web snooping can be annoying. Cookies are how a pair of pants you look at in one site end up following you around in ads elsewhere. More fundamentally, your web history – like the color of your underpants – ain't nobody's business but your own. Letting anyone collect that data leaves it ripe for abuse by bullies, spies and hackers.

Google's product managers told me in an interview that Chrome prioritizes privacy choices and controls, and they're working on new ones for cookies. But they also said they have to get the right balance with a "healthy web ecosystem" (read: ad business).

Firefox's product managers told me they don't see privacy as an "option" relegated to controls. They've launched a war on surveillance, starting this month with "enhanced tracking protection" that blocks nosy cookies by default on new Firefox installations. But to succeed, first Firefox has to convince people to care enough to overcome the inertia of switching.

It's a tale of two browsers – and the diverging interests of the companies that make them.

The cookie fight

A decade ago, Chrome and Firefox were taking on Microsoft's lumbering giant Internet Explorer. The upstart Chrome solved real problems for consumers, making the web safer and faster. Today it dominates more than half the market.

Lately, however, many of us have realized that our privacy is also a major concern on the web – and Chrome's interests no longer always seem aligned with our own.

That's most visible in the fight over cookies. These code snippets can do some helpful things, like remembering the contents of your shopping cart. But now many cookies belong to data companies, which use them to tag your browser so they can follow your path like crumbs in the proverbial forest.

They're everywhere – one study found third-party tracking cookies on 92 percent of websites. The Washington Post website has about 40 tracker cookies, average for a news site, which the company said in a statement are used to deliver better-targeted ads and track ad performance.

You'll also find them on sites without ads: Both Aetna and the FSA service said the cookies on their sites help measure their own external marketing campaigns.

The blame for this mess belongs to the entire advertising, publishing and tech industries. But what responsibility does a browser have in protecting us from code that isn't doing much more than spying?

In 2015, Mozilla debuted a version of Firefox that included anti-tracking tech, turned on only in its "private" browsing mode. After years of testing and tweaking, that's what it activated this month on all websites. This isn't about blocking ads – those still come through. Rather, Firefox is parsing cookies to decide which ones to keep for critical site functions and which ones to block for spying.

Apple's Safari browser, used on iPhones, also began applying "intelligent tracking protection" to cookies in 2017, using an algorithm to decide which ones were bad.

Chrome, so far, remains open to all cookies by default. Last month, Google announced a new effort to force third-party cookies to better self-identify, and said we can expect new controls for them after it rolls out. But it wouldn't offer a timeline or say whether it would default to stopping trackers.

I'm not holding my breath. Google itself, through its Doubleclick and other ad businesses, is the No. 1 cookie maker – the Mrs. Fields of the web. It's hard to imagine Chrome ever cutting off Google's moneymaker.

"Cookies play a role in user privacy, but a narrow focus on cookies obscures the broader privacy discussion because it's just one way in which users can be tracked across sites," said Ben Galbraith, Chrome's director of product management. "This is a complex problem, and simple, blunt cookie blocking solutions force tracking into more opaque practices."

There are other tracking techniques – and the privacy arms race will get harder. But saying things are too complicated is also a way of not doing anything.

"Our viewpoint is to deal with the biggest problem first, but anticipate where the ecosystem will shift and work on protecting against those things as well," said Peter Dolanjski, Firefox's product lead.

Both Google and Mozilla said they're working on fighting "fingerprinting," a way to sniff out other markers in your

computer. Firefox is already testing its capabilities, and plans to activate them soon.

Making the switch

Choosing a browser is no longer just about speed and convenience – it's also about data defaults.

It's true that Google usually obtains consent before gathering data, and offers a lot of knobs you can adjust to opt out of tracking and targeted advertising. But its controls often feel like a shell game that results in us sharing more personal data.

I felt hoodwinked when Google quietly began signing Gmail users into Chrome last fall. Google says the Chrome shift didn't cause anybody's browsing history to be "synced" unless they specifically opted in – but I found mine was being sent Google, and don't recall ever asking for extra surveillance. (You can turn off the Gmail auto-login by searching "Gmail" in Chrome settings and switching off "Allow Chrome sign-in.")

After the sign-in shift, Johns Hopkins professor Matthew Green made waves in the computer science world when he blogged he was done with Chrome. "I lost faith," he told me. "It only takes a few tiny changes to make it very privacy unfriendly."

There are ways to defang Chrome, which is much more complicated than just using "Incognito Mode." But it's much easier to switch to a browser not owned by an advertising company.

Like Green, I've chosen Firefox, which works across phones, tablets, PCs and Macs. Apple's Safari is also a good option on

Macs, iPhones and iPads, and the niche Brave browser goes even further in trying to jam the ad-tech industry.

What does switching to Firefox cost you? It's free, and downloading a different browser is much simpler than changing phones.

In 2017, Mozilla launched a new version of Firefox called Quantum that made it considerably faster. In my tests, it has felt almost as fast as Chrome, though benchmark tests have found it can be slower in some contexts. Firefox says it's better about managing memory if you use lots and lots of tabs.

Switching means you'll have to move your bookmarks, and Firefox offers tools to help. Shifting passwords is easy if you use a password manager. And most browser add-ons are available, though it's possible you won't find your favorite.

Mozilla has challenges to overcome. Among privacy advocates, the nonprofit is known for caution. It took a year longer than Apple to make cookie blocking a default.

And as a nonprofit, it earns money when people make searches in the browser and click on ads – which means its biggest source of income is Google. Mozilla's CEO says the company is exploring new paid privacy services to diversify its income.

Its biggest risk is that Firefox might someday run out of steam in its battle with the Chrome behemoth. Even though it's the No. 2 desktop browser, with about 10 percent of the market, major sites could decide to drop support, leaving Firefox scrambling.

If you care about privacy, let’s hope for another David and Goliath outcome.