The Washington Post

Consumer Tech Perspective

I found your data. It's for sale.

+ Add to list

As many as 4 million people have Web browser extensions that sell their every click. And that's just the tip of the iceberg.

By Geoffrey A. Fowler

I've watched you check in for a flight and seen your doctor refilling a prescription.

I've peeked inside corporate networks at reports on faulty rockets. If I wanted, I could've even opened a tax return you only shared with your accountant.

I found your data because it's for sale online. Even more terrifying: It's happening because of software you probably installed yourself.

My latest investigation into the secret life of our data is not a fire drill. Working with an independent security researcher, I found as many as 4 million people have been leaking personal and corporate secrets through Chrome and Firefox. Even a colleague in The Washington Post's newsroom got caught up. When we told browser makers Google and Mozilla, they shut these leaks immediately — but we probably identified only a fraction of the problem.

The root of this privacy train wreck is browser extensions. Also known as add-ons and plug-ins, they're little programs used by nearly half of all desktop Web surfers to make browsing better, such as finding coupons or remembering passwords. People install them assuming that any software offered in a store run by Chrome or Firefox has got to be legit.

Not. At. All. Some extensions have a side hustle in spying. From a privileged perch in your browser, they pass information about where you surf and what you view into a murky data economy. Think about everything you do in your browser at work and home — it's a digital proxy for your brain. Now imagine those clicks beaming out of your computer to be harvested for marketers, data brokers or hackers.

Some extensions make surveillance sound like a sweet deal: This week, Amazon was offering people $10 to install its Assistant extension. In the fine print, Amazon said the extension collects your browsing history and what’s on the pages you view, though all that data stays inside the giant company. (Amazon CEO Jeff Bezos owns The Washington Post.) Academic researchers say there are thousands of extensions that gather browsing data — many with loose or downright deceptive data practices — lurking in the online stores of Google and even the more privacy-friendly Mozilla.

The extensions we found selling your data show just how dangerous browser surveillance can be. What’s unusual about this leak is that we got to watch it taking place. This isn’t a theoretical privacy problem: Here’s exactly how millions of people’s data got grabbed and sold — and the failed safeguards from browser makers that let it happen.

A ‘catastrophic’ leak

I didn’t realize the scale of the extension problem until I heard from Sam Jadali. He runs a website hosting business, and earlier this year found some of his clients’ data for sale online. Figuring out how that happened became a six-month obsession.

Jadali found the data on a website called Nacho Analytics. Just one small player in the data economy, Nacho bills itself on its website as a marketing intelligence service. It offers data about what’s being clicked on at almost any website — including actual Web addresses — for as little as $49 per month.

That data, Nacho claims, comes from people who opt in to being tracked, and it redacts personally identifiable information.

The deeper Jadali looked on Nacho, the more he found that went way beyond marketing data. Web addresses — everything you see after the letters “http” — page titles and other browsing records might not seem like they’d expose much. But sometimes they contain secrets sites forget to hide away.

Jadali found usernames, passwords and GPS coordinates, even though Nacho said it scrubs personal information from its data. “I started realizing this was a leak on a catastrophic scale,” Jadali told me.

What he showed me made my jaw drop. Three examples:

From DrChrono, a medical records service, we saw the names of patients, doctors, and even medications. From another service, called Kareo, we saw patient names.

From Southwest, we saw the first and last names, as well as confirmation numbers, of people checking into flights. From United, we saw last names and passenger record numbers.

From OneDrive, Microsoft’s cloud storage service, we saw a hundred documents named “tax.” We didn’t click on any of these links to avoid further exposing sensitive data.

It wasn’t just personal secrets. Employees from more than 50 major corporations were exposing what they were working on (including top-secret stuff) in the titles of memos and project reports. There was even information about internal corporate networks and firewall codes. This should make IT security departments very nervous.

Jadali documented his findings in a report titled “DataSpii,” and has spent the last two weeks disclosing the leaks to the companies he identified — many of which he thinks could do a better job keeping secrets out of at-risk browser data. I also contacted all the companies I name in this column. Kareo and Southwest told me they’re removing names from page data.

I wondered if Jadali could find any data from inside The Washington Post. Shortly after I asked, Jadali asked me if I had a colleague named Nick Mourtoupalas. On Nacho, Jadali could see him clicking on our internal websites. Mourtoupalas had just viewed a page about the summer interns. Over months, he’d probably leaked much, much more.

I called up Mourtoupalas, a newsroom copy aide. Pardon the interruption, I said, but your browser is leaking.

“Oh, wow, oh, wow,” Mourtoupalas said. He hadn’t ever “opted in” to having his Web browsing tracked. “What have I done wrong?”

Follow the data

I asked Mourtoupalas if he’d ever added anything to Chrome. He pulled up his extensions dashboard and found he’d installed 17 of them. “I didn’t download anything crazy or shady looking,” he said.

One of them was called Hover Zoom. It markets itself in the Chrome Web Store and its website as a way to enlarge photos when you put your mouse over them. Mourtoupalas remembered learning about it on Reddit. Earlier this year, it had 800,000 users.

When you install Hover Zoom, a message pops up saying it can “read and change your browsing history.” There’s little indication Hover Zoom is in the business of selling that data.

I tried to reach all the contacts I could find for Hover Zoom's makers. One person, Romain Vallet, told me he hadn't been its owner for several years, but declined to say who was now. No one else replied.

Jadali tested the links between extensions and Nacho by installing a bunch himself and watching to see if his data appeared for sale. We did some of these together, with me as a willing victim. After I installed an extension called PanelMeasurement, Jadali showed me how he could access private iPhone and Facebook photos I'd opened in Chrome, as well as a OneDrive document I had named "Geoff's Private Document." (To find the latter, all he had to do was search page titles on Nacho for "Geoff.")

In total, Jadali's research identified six suspect Chrome and Firefox extensions with more than a few users: Hover Zoom, SpeakIt!, SuperZoom, SaveFrom.net Helper, FairShare Unlock and PanelMeasurement.

They all state in either their terms of service, privacy policies or descriptions that they may collect data. But only two of them — FairShare Unlock and PanelMeasurement — explicitly highlight to users that they collect browser activity data and promise to reward people for surfing the Web.

"If I've fallen in for using this extension, I know hundreds of thousands of other people easily have also," Mourtoupalas told me. He's now turned off all but three extensions, each from a well-known company.

BANNED EXTENSION NAME	NUMBER OF USERS	BROWSER
Hover Zoom	800,000	Chrome
SpeakIt!	1.4+ million	Chrome
SuperZoom	329,000	Chrome and Firefox
SaveFrom.net Helper†	≤140,000	Firefox
FairShare Unlock	1+ million	Chrome and Firefox
PanelMeasurement	500,000	Chrome

Source: Sam Jadali

†*The data collecting behavior occurred only in a version of the SaveFrom.net Helper installed from the author's website*

The tip of the iceberg

After we disclosed the leaks to browser makers, Google remotely deactivated seven extensions, and Mozilla did the same to two others (in addition to one it disabled in February). Together, they had tallied more than 4 million users. If you had any of them installed, they should no longer work.

A firm called DDMR that made FairShare Unlock and PanelMeasurement told me the ban was unfair because it sought user consent. (It declined to say who its clients were, but said its terms prohibited customers from selling confidential information.) None of the other extension makers answered my questions about why they collected browsing data.

A few days after the shutdown, Nacho posted a notice on its website that it had suffered a “permanent” data outage and would no longer take on new clients, or provide new data for existing ones.

But that doesn’t mean this problem is over.

North Carolina State University researchers recently tested how many of the 180,000 available Chrome extensions leak privacy-sensitive data. They found 3,800 such extensions — and the 10 most popular alone have more than 60 million users.

“Not all of these companies are malicious, or doing this on purpose, but they have the ability to sell your data if they want,” said Alexandros Kapravelos, a computer science professor who worked on the study.

Extension makers sometimes cash out by selling to companies that convert their popular extensions into data Hoovers. The 382 extensions Kapravelos suspects are in the data-sale business have nearly 8 million users. “There is no regulation that prevents them from doing this,” he said.

So why aren’t Google and Mozilla stopping it? Researchers have been calling out nefarious extensions for years, and the companies say they vet what’s in their stores. “We want Chrome extensions to be safe and privacy-preserving, and detecting policy violations is essential to that effort,” said Google senior director Margret Schmidt.

But clearly it’s insufficient. Jadali found two extensions waited three to five weeks to begin leaking data, and he suspects they may have delayed to avoid detection. Google recently announced it would begin requiring extensions to minimize the data they access, among other technical changes. Mozilla said its recent focus has also been on limiting the damage add-ons can do.

Just as big a problem is a data industry that’s grown cavalier about turning our lives into its raw material.

In an interview, Nacho CEO Mike Roberts wouldn’t say where he sourced his data. But Jadali, he said, violated Nacho’s terms of service by looking at personal information. “No actual Nacho Analytics customer was looking at this stuff. The only people that saw any private information was you guys," Roberts said.

I'm not certain how he could know that. There were so many secrets on Nacho that tracking down all the ways they might have been used is impossible.

His defense of Nacho boiled down to this: It's just the way the Internet works.

Roberts said he believed the people who contributed data to Nacho — including my colleague — were "informed." He added: "I guess it wouldn't surprise me if some people aren't aware of what every tool or website does with their data."

Nacho is not so different, he said, from others in his industry. "The difference is that I wanted to level the playing field and put the same power into the hands of marketers and entrepreneurs — and that created a lot more transparency," he said. "In a way, that transparency can be like looking into a black mirror."

He's not entirely wrong. Large swaths of the tech industry treat tracking as an acceptable way to make money, whether most of us realize what's really going on. Amazon will give you a $10 coupon for it. Google tracks your searches, and even your activity in Chrome, to build out a lucrative dossier on you. Facebook does the same with your activity in its apps, and off.

Of course, those companies don't usually leave your personal information hanging out on the open Internet for sale. But just because it's hidden doesn't make it any less scary.

Read more tech advice and analysis from Geoffrey A. Fowler:

Die, robocalls, die: A how-to guide to stop spammers and exact revenge

Not all iPhones are the same. These cost less and are better for the Earth.

Rock this way: AirPods, Beats and Bose wireless ear buds take the headbang test

Geoffrey A. Fowler
Geoffrey A. Fowler is The Washington Post's technology columnist based in San Francisco. He joined The Post in 2017 after 16 years with the Wall Street Journal writing about consumer technology, Silicon Valley, national affairs and China. Follow