Democracy Dies in Darkness

Meta found a new way to violate your privacy. Here’s what you can do.

Even hardened digital privacy veterans said they were stunned by Meta’s tactics.

June 6, 2025

Analysis by Shira Ovide

Researchers recently caught Meta using tactics that one expert called similar to those of digital crooks to secretly compile logs of people’s web browsing on Android devices.

No one, including Android owner Google, knew that Meta’s Facebook and Instagram apps were siphoning people’s data through a digital back door for months. (After the researchers publicized their findings, Meta said it stopped.)

It’s not novel that Meta is undermining your privacy. But the tactics the researchers identified were so scuzzy they surprised even those digital privacy experts who have seen every trick in the book.

“It’s such a gross violation of people’s basic expectations,” said Peter Dolanjski, a product director for DuckDuckGo, which makes a privacy-focused web search engine and web browser.

I’ll explain how researchers found Meta’s tricks and suggest a few ways to safeguard your digital privacy.

This episode, though, is bigger than just one company. The research findings show that even after years of revelations about companies turning your phone into an always-on surveillance device, the problems are maddeningly persistent.

Unraveling a Meta mystery

Gunes Acar, an assistant professor at Radboud University in the Netherlands, noticed something odd when he was on the university’s website looking for course materials about online tracking and privacy.

Millions of websites contain a string of computer code from Meta that compiles your web activity. It might capture the income you report to the government, your application for a student loan and your online shopping.

Meta uses logs from this Meta Pixel software to build a profile of you for advertising.

Shira Ovide

Tech Friend writer Shira Ovide gives you advice and context to make

technology work for you. Sign up for the free Tech Friend newsletter.
Contact her securely on Signal at ShiraOvide.70

(Patrick Dias for The Washington Post)

Typically, Acar said, information from this Meta software flows one way: It connects once to your computer to send data to Meta’s cloud. But Acar watched the Meta Pixel software try to reconnect to his computer, which he altered to impersonate a web browser on an Android device.

To unravel this puzzling behavior, Acar enlisted collaborators at the Computer Security and Industrial Cryptography research group at Belgian university KU Leuven and IMDEA Networks, a research institute in Spain.

Ars Technica wrote a technical analysis, but the gist is that researchers found that apps from Meta and Yandex, a technology company that originated in Russia, circumvented privacy protections in Android devices in ways that allowed their apps to secretly track people as they browsed the web.

That should not have happened. Apps on your phone are walled off from accessing your activity on other apps, including web browser apps like Chrome. Meta and Yandex found work-arounds.

The techniques essentially were akin to malware, or malicious software that is surreptitiously planted on your phone or computer, Dolanjski said.

Google said the behaviors of Meta and Yandex “blatantly violate our security and privacy principles.”

A Meta representative said the company is talking to Google “to address a potential miscommunication regarding the application of their policies.” Meta said it paused what it was doing.

Yandex said it did not “collect any sensitive information.” It, too, said the company has stopped the practice the researchers identified.

If you’re wondering about iPhones, the research team said it doesn’t have evidence of Meta and Yandex doing similar backdoor data-harvesting on Apple devices. The researchers said it could be technically feasible and plan to investigate further. An Apple spokesperson didn’t comment.

Albert Fox Cahn, executive director of the Surveillance Technology Oversight Project, a consumer privacy advocacy group, said that “we should be outraged” at the researchers’ findings.

What you can do to protect your privacy

No privacy setting could have stopped what Meta and Yandex did. They circumvented privacy and security protections that Google set up for Android devices.

But their tactics underscored some privacy vulnerabilities in web browsers or apps. These steps can reduce your risks.

Stop using the Chrome browser. Mozilla's Firefox, the Brave browser and DuckDuckGo's browser block many common methods of tracking you from site to site. Chrome, the most popular web browser, does not.

If you have an Android phone, you can change your phone settings to make one of those more privacy-preserving browsers the default anytime you click a web link.

For iPhone and Mac folks, Safari also has strong privacy protections. It's not perfect, though.

No browser protections are foolproof. The researchers said Firefox on Android devices was partly susceptible to the data harvesting tactics they identified, in addition to Chrome. (DuckDuckGo and Brave largely did block the tactics, the researchers said.)

Opt for a company's website over its app when it makes sense. Compared with apps, websites cannot track you as easily nor access your confidential information without permission.

So if you do something on your phone only occasionally — buying plane tickets or shopping for home insurance — you typically have more privacy protections if you use the company's website rather than its smartphone app.

Delete Meta and Yandex apps on your phone, if you have them. The tactics described by the European researchers showed that Meta and Yandex are unworthy of your trust. (Yandex is not popular in the United States.)

It might be wise to delete their apps, which give the companies more latitude to collect information that websites generally cannot easily obtain, including your approximate location, your phone's battery level and what other devices, like an Xbox, are connected to your home WiFi.

Know, too, that even if you don't have Meta apps on your phone, and even if you don't use Facebook or Instagram at all, Meta might still harvest information on your activity across the web.

Read more:

- Change these Facebook privacy settings right now
- Yeah, your phone is listening to you. But probably not to target ads.
- This is the best privacy settings that almost no one is using.

What readers are saying

What readers are saying

The comments express significant concern over the privacy implications of Meta and Yandex's tactics, with many users criticizing the invasive data collection practices and lack of accountability. There is a strong sentiment that these actions are criminal and should be met with... Show more

This summary is AI-generated. AI can make mistakes and this summary is not a replacement for reading the comments.