The Washington Post
Democracy Dies in Darkness

Facebook will now show you exactly how it stalks you — even when you're not using Facebook

The new 'Off-Facebook Activity' tool reminds us we're living in a reality TV program where the cameras are always on. Here are the privacy settings to change right now.

By **Geoffrey A. Fowler**

Jan. 28, 2020 at 8:35 p.m. EST

Ever suspect the Facebook app is listening to you? What we now know is even creepier.

Facebook is giving us a new way to glimpse just how much it knows about us: On Tuesday, the social network made a long-delayed "Off-Facebook Activity" tracker available to its 2 billion members. It shows Facebook and sister apps Instagram and Messenger don't need a microphone to target you with those eerily specific ads and posts — they're all up in your business countless other ways.

Even with Facebook closed on my phone, the social network gets notified when I use the Peet's Coffee app. It knows when I read the website of presidential candidate Pete Buttigieg or view articles from The Atlantic. Facebook knows when I click on my Home Depot shopping cart and when I open the Ring app to answer my video doorbell. It uses all this information from my not-on-Facebook, real-world life to shape the messages I see from businesses and politicians alike.

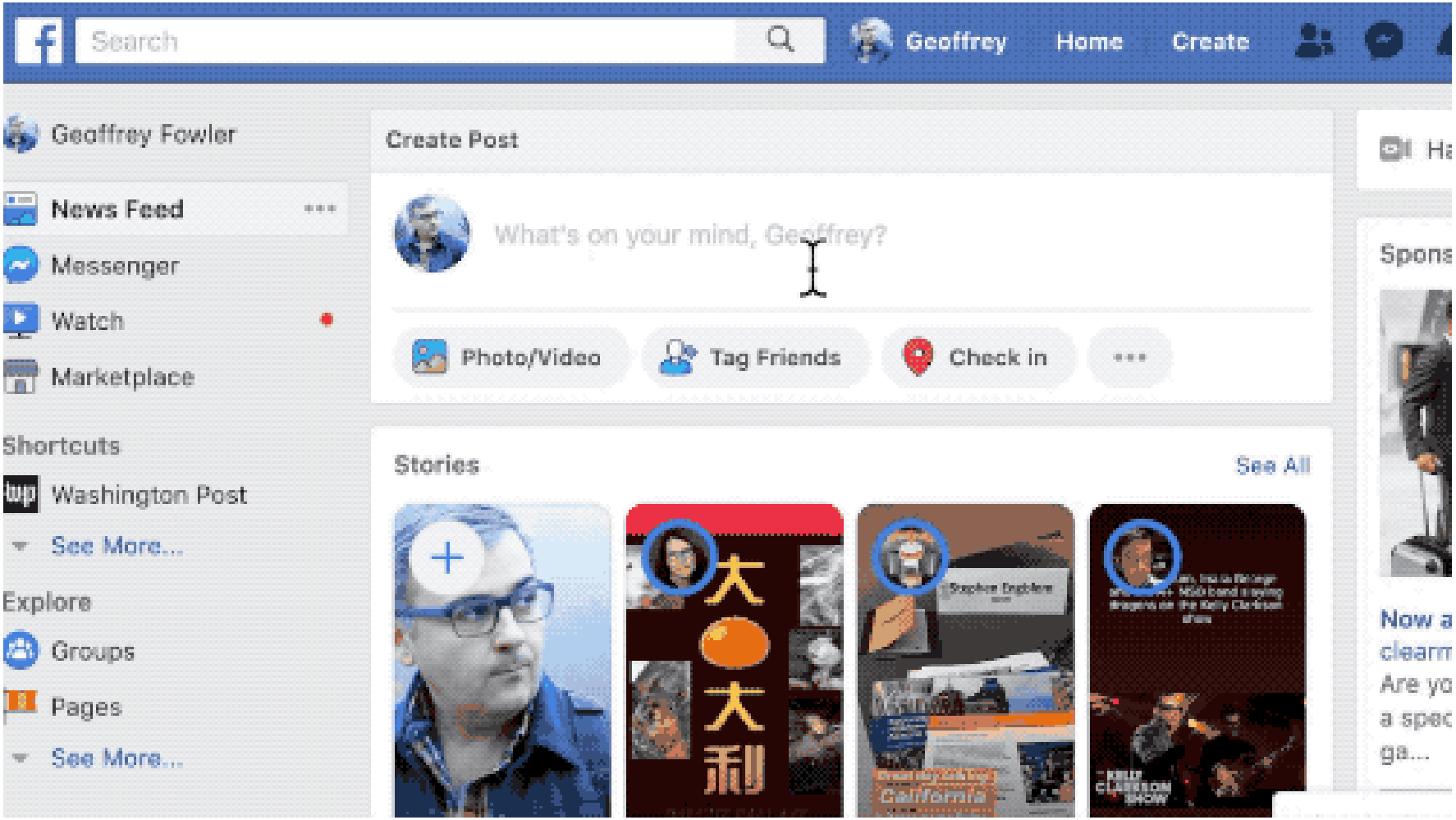
You can see how Facebook is stalking you, too. The "Off-Facebook Activity" tracker will show you 180 days' worth of the data Facebook collects about you from the many organizations and advertisers in cahoots with it. This page, buried behind lots of settings menus (here's a direct link), is the product of a promise CEO Mark Zuckerberg made during the height of the 2018 Cambridge Analytica scandal to provide ways we can "clear the history" in our accounts.

Facebook's new tool isn't nearly as useful as your Web browser's clear-history button — it doesn't let you reset your entire relationship with Facebook. But along with the transparency, it does give you a way to unlink some of its surveillance from your Facebook account.

(Click here to jump to the part of this column where I show you how.)

You might be shocked or at least a little embarrassed by what you find in there. My Post colleagues found that Facebook knew about a visit to a sperm-measurement service, log-ins to medical insurance and even the website to register for the Equifax breach settlement. Even when your phone is entirely off, businesses can upload information about you making an in-store purchase. One colleague found 974 apps and websites shared his activity.

There's not necessarily a new privacy violation here. Facebook has been partnering with websites, apps and stores to track and target customers for years. And it's hardly alone. Lots of companies send information about us to ad and data firms. Think of it more as a reminder that we're all living in a reality TV program where the cameras are always on.



To see what information Facebook has collected about you from other apps, websites and businesses, go to Settings, then Your Facebook Information, then Off-Facebook Activity.

Anyone who's concerned about the power Facebook has to manipulate people and shape elections should care about how it tracks us. It's easy to forget in the constant barrage of Zuckerberg's privacy apologies and fines, but here's the reality: Facebook keeps gathering more and more data about us, with few laws restricting how it can use it.

Rivals such as Google don't offer anything comparable to the "Off-Facebook Activity" page.

"Despite how commonplace this activity is across the Internet, we believe it's important to help people understand why they're seeing the ads they see and to give them control over how their data is used, regardless of the services they use," says Facebook spokesman Jay Nancarrow.

But hold the applause: Laws such as this year's California Consumer Privacy Act require companies to let us know exactly what data they've collected about us.

Regardless, I'll take Facebook's new tool as a win for us. It offers an opportunity to see in ugly detail how Facebook's advertising surveillance system actually works. Chances are, it's not at all like you think.

Why are you seeing that ad?

If all of this sounds confusing, it's not your fault. A Pew survey published in 2019 found 74 percent of American Facebook members were unaware that the social network builds a dossier on each of us to target ads. Facebook makes its surveillance systems so convoluted and, frankly, boring that we're less likely to object. I'm not letting that stop me.

Here's the big picture: Everybody's experience on Facebook and Instagram is different. Your feed might be filled with stories about luxury real estate and ads from Mike Bloomberg, while mine might be NASCAR and President Trump commercials. That's because Facebook's software uses the data it gathers about us to tailor what it shows us. Facebook also lets advertisers target messages to the people the data suggests might be most receptive — or, in the case of political advertisers, easily swayed.

Facebook uses some data to put you into "interest" categories, such as people who live in Washington and are into cats. You can see the boxes Facebook has put you in by looking under its "ad preferences" menus. (Click here for a direct link to view and, if you want, delete some of these categories.)

A part of this is easy to understand. Facebook obviously knows who your friends are, what you "like," and what and where you post. You entered that information yourself.

But there's also a world of information Facebook gathers that you didn't volunteer to the social network — and probably didn't know was being collected.

How does Facebook get this info? The social network provides partners tracking software they embed in apps, websites, loyalty cards and other systems. According to research by the Electronic Frontier Foundation, Facebook has so-called tracker pixels or cookie-sharing code on about 30 percent of the top 10,000 websites.

Facebook's surveillance is hard to avoid. It doesn't require you to click "like" or use a "login with Facebook" button. You don't necessarily have to be logged in to the Facebook app or website on your phone — companies can report other identifying information to Facebook, which will marry up the activity to your account after the fact.

Your off-Facebook activity isn't exposed to your friends; they won't see it in the News Feed. The social network also doesn't pass your personal information back to businesses — they just get the chance to target ads to people with Facebook accounts who triggered the trackers. A company could, for example, ask Facebook to show ads to people who looked at a certain style of shoe. (Off-Facebook activity doesn't contribute to Facebook's dossier of your ad "interests," but the social network might use it to suggest groups, events or Marketplace items to buy.)

Thanks to the "Off-Facebook Activity" tool, I now know that Home Depot told Facebook when I visited its online store, viewed an item or added an item to a shopping cart. The Atlantic shared the pages I viewed and devices I used, which it says inform its distribution strategy and help it target campaigns. The Washington Post says it stopped using the Facebook tracking pixel, along with some other social-networking trackers, on content pages as of Oct. 24.

The Buttigieg campaign says it used the Facebook tracking pixel to target ads at people who have visited its website or engaged with its donation link. Peet's Coffee didn't respond to my questions.

Ring, which is owned by Amazon, let Facebook know when I installed or opened its app. Spokeswoman Yassi Shahmiri says Ring uses the information to "optimize our marketing campaigns on Facebook," including advertising less to people who already own the product.

But is that a good reason to share information about my doorbell with Facebook? Shahmiri says Ring doesn't share specific camera data, such as a motion detected at your door. But Ring does ping Facebook when I open the app, which is almost always when there's someone at my door. Guess I was foolish to presume what happens on my doorstep stays between me and Ring. (Amazon CEO Jeff Bezos owns The Washington Post, but I review all tech with the same critical eye.)

Facebook says it puts limits on the information organizations can share with it. For example, they're not supposed to pass along health and financial information. But it's unclear how well Facebook polices this. Using forensic software, I found Facebook tracker code on the website for an HIV drug. Nancarrow, the Facebook spokesman, says that "a health site with a Facebook Pixel does not mean that they are sharing sensitive medical information with Facebook."

Don't businesses worry we'll find this to be oversharing? Most probably never thought we'd find out. Facebook says companies are required to provide us "robust notice" that they're sending data about our activity to the social network. But I found that very few explained this tracking in clear terms.

Facebook wants to paint surveillance as totally normal. Zuckerberg often says people want to see "relevant" ads. I wonder whom he's asking. About 81 percent "of the public say that the potential risks they face because of data collection by companies outweigh the benefits," according to Pew.

What you can do

You can do a few things to fight back against Facebook's surveillance, some of which haven't been available before.

The new "Off-Facebook Activity" page includes ways to ask Facebook to cut it out. From that page, click on "Clear History" to tell Facebook remove that data from your account.

After you've done that, you still need to inform Facebook you want them to stop adding this data to your profile in the future. On the same "Off-Facebook Activity" page, look for another option to "Manage Future Activity." (To find it, you may first have to click "More Options" — sorry, I know they're not making this easy.) Click that, and then click the additional button labeled "Manage Future Activity," and then toggle off the button next to "Future Off-Facebook Activity."

An important caveat: Turning off your off-Facebook activity will mean losing access to apps and websites you've used Facebook to login to in the past. (Aside from privacy concerns, there are also security reasons why Facebook logins are a bad idea.)

While we're adjusting things, I also recommend changing one other bad Facebook default setting. Under the settings menu, go to "Your Ad Preferences" (click here to go directly). Under the heading "Ad settings," look for "Ads based on data from partners." Make sure it is set to "Not allowed."

Now I have to share a bummer: Changing these settings doesn't actually stop Facebook from collecting data about you from other businesses. Facebook will just "disconnect" it from your profile, to use the social network's carefully chosen word. Mostly they're just promising they'll no longer use it to target you with ads on Facebook and Instagram — which means you'll be less likely to be manipulated based on your data. (Facebook has separately said that starting this summer we will be able to adjust a setting to see fewer political and social issue ads on Facebook and Instagram.)

So what can you do if you don't want Facebook collecting all this data about you in the first place? That requires more hand-to-hand combat.

On your computer, use a Web browser that fights trackers, like Mozilla's Firefox. Or go even further by adding an ad or tracking-blocking extension to your browser, such as the EFF's Privacy Badger. My account tallied much less off-Facebook activity than most of my colleagues because I use Firefox along with Mozilla's Facebook Container add-on, which prevents Facebook's software from connecting with other sites.

In smartphone apps, where tracking is also increasingly common, tracking even is harder to stop. A few services, such as Disconnect's Privacy Pro, scan app activity and block tracker traffic, but they may also interfere with the way apps function.

Or there's the ultimate fix: Say farewell to Facebook and Instagram forever, and close your accounts. So far, though, that's not a choice most people have been willing to make.

Read more from our Secret Life of Your Data series:

Alexa has been eavesdropping on you this whole time

It's the middle of the night. Do you know who your iPhone is talking to?

The spy in your wallet: Credit cards have a privacy problem

Goodbye, Chrome: Google's Web browser has become spy software

I found your data. It's for sale.

You watch TV. Your TV watches back.

Think you're anonymous online? A third of popular websites are 'fingerprinting' you.

What does your car know about you? We hacked a Chevy to find out.

How we survive the surveillance apocalypse
