New American

Written by **C. Mitchell Shaw** on April 23, 2022

Yes, Your Mobile Carrier Is Probably Spying on You, But You Can Do Something About It

Roman Stavila/iStock/Getty Images Plus

In the world that exists after Ed Snowden's 2013 revelations, it is well-known that government agencies routinely spy on American citizens. But many seem to not know that tech companies make large profits doing the same and selling private data to advertisers.

That ignorance is on full display in an article published in the *Washington Post's* "Help Desk" section on April 22. Tatum Hunter answers a query from a reader about whether or not mobile carriers harvest users' data for profit. She admits, "I had no idea wireless carriers were in the business of peeking in on my activities and using that information to market to me."

Her admission comes in the wake of her discovery that such surveillance is a common business practice in the industry. She writes:

> At Help Desk, we read privacy policies so you don't have to. This week, a curious reader inspired us to dive deeper into cell carriers (thanks, Ron from Houston!). I read privacy policies from the three major wireless carriers — Verizon, AT&T and T-Mobile — and my eyeballs are only bleeding a little. All three carriers have some less-than-great privacy practices hiding in plain sight. Depending on the carrier, they can draw on your Internet history, app use, location and call history to learn things about you and nudge you to spend more money on products from themselves or third-party companies.

Hunter mentions Verizon's "Custom Experience" as an example of such programs. But she also points out that other companies have similar programs. It turns out that surveillance is big business for mobile carriers. And since *literally* everything people do on their mobile phone is passed through their carriers' networks, everything is within their reach. Browsing, messages, e-mails, calendars, maps, notes, and more are sent straight from your phone to your carrier.

At least that is the default.

But though the *Washington Post's* Help Desk seems to have finally figured out that mobile carriers make big bucks snooping on their customers' data, they have not yet figured out that simply asking your provider not to is not enough. Hunter writes, "Some good news: You can opt out whenever you want, and we're going to show you how." She describes the process for "opting out," writing:

> Verizon customers appear to be automatically opted into the company's "Custom Experience" program, which means the company can use your browsing history and data

> from your apps to help target ads. The company says it "makes efforts" not to target you based on adult sites you visit, health conditions and sexual orientation. (Thanks, Verizon.) If you said "yes" to "Custom Experience Plus" at any point, the company can also use your location and call logs.
>
> AT&T's "Relevant Advertising" program works similarly. Customers are automatically opted in, and the company draws on information including your browsing history and videos you've watched to help show you targeted ads. If you sign up for "Enhanced Relevant Advertising," your device location and call history are also fair game.
>
> In comparison, T-Mobile's data-crunching seems relatively tame: It says it doesn't use any web-browsing, precise location or call history data for its ad program, but it can use your "mobile app usage" and video-viewing data, according to its website.

And:

> Verizon customers can opt out of Custom Experience by going to their privacy settings in the My Verizon app or by following this link. (While you're there, check that you haven't said yes to "Custom Experience Plus," either.)
>
> AT&T customers can opt out by signing into att.com, navigating to the "AT&T Consent Dashboard" and scrolling to the section "Control how we use your data." (Or follow this link.) Opt out of "Relevant Advertising" and check that you're not signed up for "Enhanced Relevant Advertising."
>
> T-Mobile says customers can opt out this way: In the app, go to More -> Advertising & Analytics -> Use my data to make ads more relevant to me. Turn the toggle off so that it turns gray. On the website, go to My Account -> Profile -> Privacy and Notifications -> Advertising & Analytics -> Use my data to make ads more relevant to me. Turn the toggle off.

It would be nice if it were that easy. But that assumes that the company that opted you into being spied on without any clear consent is simply going to stop harvesting your data just because you asked. Perhaps they will, but this writer thinks not. Call me jaded, but if a company is making jillions of dollars stealing your data, I find it hard to believe that asking them to stop comes with any assurance they will. Besides that, your carrier is not the only company spying on your mobile traffic. Other companies — including app developers, websites, and those offering "free WiFi" — harvest your data as well.

However, to borrow a phrase from Hunter, "Some good news: You can opt out whenever you want, and we're going to show you how." And no, it is not by asking your carrier to do something they should not be doing in the first place.

The simple truth is that it is *your* data and *you* are going to have to protect it. I recommend a few simple steps. First, keep your devices and apps up-to-date. Security vulnerabilities arise and phone manufacturers, carriers, and app developers issue patches to close those vulnerabilities. If you get an update, install it.

Also, pay attention to all app permissions and do not install *any* app that asks for permissions it should not need. A calculator app, for instance, should not need to see your contacts or call log. You get the

idea — ask yourself, “Does this app *need* that permission to do what I want it to do?” If not, find another app that does the same thing but without asking for hinky permissions.

Next, slim down on your apps. If you are like most people, you have three times the apps you will ever use, and most of them you *never* use. Delete them. Less is more.

Speaking of apps, avoid social media apps on your phone. If you must use social media, use it in the browser. The apps are notorious for leaking data back to the company that created the app. Sure, the mobile version of social media sites offers fewer features, but there are two important points to observe about that fact. First, those companies could easily build the same features into their mobile sites as they do in their desktop sites and apps. So, why don’t they? Because they want you to need the app so that they have greater access to your device. Second, if you are out and about, you *may* feel that you need to check your social media feeds (you probably don’t *need* to, but you *think* you do), but the mobile site in the browser will at least give you the bare-bones experience. After a while, you likely won’t miss the apps at all.

The next step in keeping your data safe is to only connect to trusted networks. That means that “free WiFi” that just pops up when you are shopping at the mall is out. Unless you know who controls the network, don’t trust it with your data.

One app you *should* consider installing is a trustworthy VPN. Essentially, a VPN (Virtual Private Network) reroutes all of your data through a network *other* than your carrier or WiFi. But beware: not all VPNs are created equal. Since you connect to the VPN, the company running that VPN could have the keys to your digital kingdom. A good rule of thumb is that “free” VPNs are simply spyware. But a good VPN — one that is operated by a trusted company and encrypts your data before sending it from your device — is different. One example is ProtonVPN — a product of the same company that offers ProtonMail. ProtonVPN is end-to-end encrypted using zero-knowledge protocols. That means that not even the folks at Proton have access to the un-encrypted data. Another benefit of using a good, trustworthy VPN is that if you *do* need to use a “free” WiFi connection, your traffic is gibberish even to the people who own the router.

Those steps should go a long way to keeping your data in your hands. As long as there is a profit to be made spying on people’s data, there will be people and companies who will do that spying. Take back control of your data by protecting it yourself. And, with one final nod to the *Washington Post’s* Help Desk, go ahead and click all those “opt out” buttons if it makes you feel better. It likely won’t help, but it won’t hurt, either. Oh, and forget Hunter’s plug for Help Desk reading privacy policies “so you don’t have to.” It’s *your* privacy — read the policies yourself.