Silicon Valley created the evil surveillance apocalypse

Geoffrey A. Fowler, The Washington Post

-
-
-
-
-
-
-
-
- FILE - In this April 11, 2018, file photo, Facebook CEO Mark Zuckerberg pauses while testifying before a House Energy and Commerce hearing on Capitol Hill in Washington about the use of Facebook data to target American voters in the 2016 election and data privacy. A year ago, Shoshana Zuboff dropped an intellectual bomb on the technology industry. In a 700-page book, the Harvard scholar skewered tech giants like Facebook and Google with a damning phrase: “surveillance capitalism.” Photo: Andrew Harnik, AP / Copyright 2018 The Associated Press. All rights reserved.

Photo: Andrew Harnik, AP
FILE - In this April 11, 2018, file photo, Facebook CEO Mark Zuckerberg pauses while testifying before a House Energy and Commerce hearing on Capitol Hill in Washington about the use of Facebook data to target American voters in the 2016 election

and data privacy. A year ago, Shoshana Zuboff dropped an intellectual bomb on the technology industry. In a 700-page book, the Harvard scholar skewered tech giants like Facebook and Google with a damning phrase: “surveillance capitalism.”

"Go, go gadgets" has long been the attitude in my house. Perhaps yours, too: A smartphone made it easier to stay in touch. A smart TV streamed a zillion more shows. A smart speaker let you talk to a smart thermostat without getting out of bed. That's progress, right?

Now I've got a new attitude: It's not just what I can get out of technology - I want to know what the technology gets out of me.

For the past year, I've been on the trail of the secret life of our data. What happens when you put your iPhone to sleep at night? Does Amazon's Alexa eavesdrop on your family? Who gets to know where you drive - and where you swipe your credit card?

Trying to get straight answers has been, literally, a full-time job. I've digested the legal word salad of privacy policies, interrogated a hundred companies and even hacked into a car dashboard to grab my data back. There are lots of stories about online threats, but it feels different watching your personal information streaming out of devices you take for granted. This year I learned there is no such thing as "incognito." Just stepping out for an errand, I discovered, lets my car record where I shop, what I listen to and even how much I weigh.

Learning how everyday things spy on us made me, at times, feel paranoid. Mostly, my privacy project left me angry. Our cultural reference points - Big Brother and tinfoil hats - don't quite capture the sickness of an era when we gleefully carry surveillance machines in our pockets and install them in our homes.

With each discovery, I've looked for ways to change my own relationship with technology. I've stopped installing new smart-home devices that let corporations or police log what's happening at my house. I switched web browsers and credit cards. When possible, I use a pseudonym or a throwaway email address.

Still, I'm going to level with you. After a year of wrestling my data from corporate America, I hardly feel in control. Being paranoid isn't enough to save us in the age of surveillance.

But no, privacy isn't dead. A path to reclaiming it - fuzzy and almost too late - is starting to emerge. We just have to be angry enough to demand it.

- Data is power

While we're busy living increasingly online lives, it's hard to know what's at stake in our data.

Most of the headlines focus on leaks and the unintended consequences of data collection, like hackers stealing credit card numbers. You hear about creepy but vague violations, like when Apple and Amazon hired people to review recordings taken from their voice assistants. In a world where so many others are collecting our personal data, it's legitimate to worry whether they're doing enough to protect it.

But there's a more fundamental problem: Why is so much of our information being collected in the first place?

When I began my privacy project, I learned something about the now-ubiquitous Alexa I hadn't quite understood when I first brought home an Echo speaker. Every time Amazon's artificial intelligence activates, it keeps a recording. Amazon had four years of my family's conversations.

There's more: Amazon also keeps reports on appliances you connect to Alexa - in my smart home, every flip of a light switch or adjustment on the thermostat. Last week, Amazon reported that Alexa users received "millions" of doorbell and motion announcements during the 2019 holiday season, "from carolers to delivery drivers and holiday guests." Surveilling that many homes is a thing the company brags about. (Amazon CEO Jeff Bezos owns The Washington Post, but I review all technology with the same critical eye.)

Amazon isn't building its dossier on you just to be creepy. It wants your voice and your data to train its AI, the technology it hopes will rule our future economy.

While we've been wondering at the new capabilities of connected apps and devices, many of them have been quietly turning our private experiences into their raw materials. These companies act like the data belongs to them, rather than us. Largely unhindered by law, a hidden economy of data brokers gobbles every data morsel it can. Author Shoshana Zuboff gave this data grab a sharp name that I hope sticks: "surveillance capitalism."

There are lots of ways your data can, and will, be used against you. Governments frequently compel companies to hand over what they know. Tracking your credit card lets retailers know how much you're willing to pay. Tracking what you watch on TV lets politicians micro-target your fears. Tracking your web surfing lets marketers glimpse your desires - to get you to buy things you may not really need.

These corporations understand that data is a form of power. It's time to take ours back.

- The arms race

Opting out is more easily said than done.

I tried putting my Alexa speaker on mute, but that defeated the purpose of having a voice-operated assistant in my house. Turning it back on, Amazon would let me delete its recordings of my voice and smart-home activity - but only after the fact, and if I remembered.

Around every corner in my connected life lay one of these traps. Data-collecting companies, especially when they're trotted in front of lawmakers, like to say they give us "control." But often it's a false choice between forgoing some new capability vs. letting them mine your life. That's not how technology has to work.

In my privacy project, I found that every swipe or tap of a credit card lets as many as a half-dozen kinds of companies grab information about what, where and how much we spend. Since I can't live without a credit card, I switched most of my purchases to the new Apple Card, which restricts its bank, Goldman Sachs, from selling customer data.

That's good, but Apple didn't do anything to stop data collection by the Mastercard network its card runs on, or by retailers and point-of-sale system operators. Sometimes companies say they protect our privacy, but I find they often use a narrow definition of privacy. Same for your smartphone: Apple brags, "What happens on your iPhone stays on your iPhone," but doesn't stop app makers from sending your personal information to third-party tracking companies.

Facebook, Google and lots of other data-collecting companies offer privacy control panels that hardly anybody ever uses. I don't blame anyone for keeping away: I've tried adjusting the terrible default settings for Google, Facebook and Amazon, but the companies keep changing the controls and the types of information they collect. Using a virtual private network, or VPN, doesn't do much to stop them from grabbing data from a device you use while logged in to one of their services.

The arms race is exhausting. After I discovered how much Google's Chrome let tracking cookies ride shotgun while I browsed the web, I switched to Mozilla's Firefox, which has default cookie-tracking protection. But even it struggles to defeat a newer, more pernicious form of tracking called fingerprinting, already used on a third of the most-popular sites.

The truth is, most of us don't have the time or expertise to defend ourselves from the smartest minds in Silicon Valley, many of whom say they want to improve the world but hooked their own financial success onto grabbing as much data as possible.

- Data co-pilots

We won't regain our privacy if we leave it up to individuals. If we're going to survive the age of surveillance, we're going to need help.

That starts with laws. Privacy isn't just an individual right. It's a public good that, when done right, keeps everyone safe, whether they're paying attention or not. This ought to be obvious: Our data shouldn't have a secret life.

America doesn't have a broad privacy law, like Europe's General Data Protection Regulation, or GDPR. But after years of U.S. lawmakers just talking about data, we're starting to see some action. So far, that has come mostly in the form of regulatory fines. We should demand laws that not only require companies to come clean about what they're taking but also place some limits on it.

Starting in January, California will bring us closer to a general data law with its new California Consumer Privacy Act, or CCPA. It treats our data like we own it, and gives California residents new powers to demand that companies show us what they've collected and who they share it with. It might force some (but not all) of the companies I investigated in my privacy project to open up.

Transparency means that vigilant citizens - and pushy journalists - can hold companies accountable through public debate about what sorts of data collection are acceptable. Transparency is also good for business: It helps consumers trust what's happening behind the digital curtains.

But better seeing our data gets us only so far. My inbox is already flooded with updated privacy policies and data disclosures from companies rushing to comply with the CCPA. Managing all the data I generate is more than even I can handle.

When we're sick, we go to a doctor. To keep our computers safe, we install anti-virus software. We rely on professionals to help out with lots of complex aspects of modern life: Why not have professionals help with data, too? Call them your privacy co-pilot.

A fledgling privacy service called Jumbo shows what's possible. From your phone, it logs into Google, Facebook, Amazon and others and spruces up your privacy on your behalf. In clear language and colorful illustrations, it explains the real choices we have and makes recommendations like you'd get from a really clued-in friend. It's my favorite app of the year.

The first time I used Jumbo, I was shocked that it identified a half-dozen privacy settings for Facebook and Google that even I had missed. Now the app goes in on a regular basis and deletes my Alexa recordings, Google data and Twitter posts, reducing the data trail I leave behind me.

Right now Jumbo is tiny and faces an uphill battle when it adds a paid version in the coming months. But the privacy co-pilot market is burgeoning with new ideas, joining the likes of password managers and security-focused WiFi routers. California's new law smartly carves out protection for third parties to manage our data for us. Now we need clear professional rules for how these companies represent us and prove their trustworthiness.

I don't know exactly how this will evolve. But we're more likely to win when there are laws that stop data collection from being a secret - and when we have companies fighting to protect our privacy, not just exploit it.