Your Data Is Way More Exposed Than You Realize

Geoffrey A. Fowler

Updated May 24, 2017 7:32 p.m. ET

Privacy wasn't a concern for her until it was too late.

The woman, who agreed to share her story if she weren't to be identified, told me she left home one midnight, after four years in a relationship. She moved away and restarted her life. But then, she says, she was bombarded by phone calls from men soliciting her for sex. Then came bizarre friend requests on social media. She says one man showed up at her house.

She suspected her ex of stalking her online, and posting her information to fuel harassment. "It is psychological torture," she told me.

She turned to a domestic-violence shelter for technical and legal help, including working with Verizon in an effort to unmask some of the phone numbers she'd logged as harassing, and helping her file for her state's "Safe at Home" status, which would shield her address from public records.

Her nightmare, which is ongoing, might not resemble your life or mine. But it's a stark reminder that erosion of privacy is a cancer of digital life. And while we might not talk about privacy as often as the latest cool app, it's only getting worse.

I hear this all the time: "I have nothing to hide." The truth is, pretty much everybody does something online they have reason to keep private. You can't see the future. The woman I spoke to said she never planned on getting into what she described as a terrible relationship.

What has your web browser seen that could embarrass you later? This isn't just about porn. Have you hunted for a new job, streamed the ball game at work, investigated a crush or googled the morning-after pill? Imagine having a report about it show up on the desk of your boss, spouse or legal adversary. The most innocuous fragments of your digital life— Facebook posts, even the Find My iPhone app—can be weaponized to target or harass.

Meanwhile, data aggregators send their bots to collect anything and everything they can about you: addresses, browsing habits, even estimated net worth. Then they glue it all together, facts and wild guesses alike, into dossiers. That's the legal side of data collection. Things get scarier when your tax accountant, credit-card company or email provider gets hacked.

Think about what's coming in the era of artificial intelligence. Many of Silicon Valley's smartest minds are making billions mining you. Since 2010, the ad industry fueled by all that data has tripled in size in the U.S. alone to an estimated $83 billion in 2017, according to eMarketer. And this year, the Federal Communications Commission changed its rules to allow your internet service provider in on the action.

OK, maybe you don't mind that underwear ad that follows you around the web. But data brokers now combine information from multiple sources to segment us in ways that go well beyond advertising. Should you be invited to join a club? Or a clinical trial?

It's about self-determination. "If people don't have the ability to control or understand how their data is being used, it can lead to severe difficulties," says Julie Brill, a former FTC commissioner and current partner at the law firm Hogan Lovells, who helped lead a big investigation of data collectors.

Many assume the law will intervene when data might be used to harm you, and they're both right and wrong. There are laws, Ms. Brill points out, but they're fairly focused on topics like health and financial data.

The Privacy Test

I have a theory: People would care a lot more about privacy if they realized how exposed they already are.

So I invited a half-dozen volunteers I hadn't met before into my lab to see how much extremely personal information I could find

about each of them in under an hour.

I managed to shock every person. It wasn't even very hard.

Level one was calling up what's out there and totally public. Lots of people have googled themselves, but fewer are familiar with "people search engines" like FamilyTreeNow.com and Spokeo, which pull together and cross-reference public data, such as property records and court reports, into one place. Anyone can use them to look for birth dates, current and former addresses, phone numbers, gobs of relatives—even ex-lovers and roommates.

Along with some legit uses—finding lost relatives, protecting against fraud—all that info could be used for "doxing," where harassers surface personal information to intimidate their targets. This public personal data could also be used to impersonate you. FamilyTreeNow.com and Spokeo accept requests to remove data, though they don't promise your name won't show up again in the future.

Everybody knows about privacy on social media, right? The problem is, people aren't very good at using privacy controls.

A site with the terrifying name StalkScan.com drives home the point. Made by a self-described "ethical hacker" named Inti De Ceukelaire, the site lets non-friends search your Facebook account for public posts, as well as public pictures, tags and likes. The founder says the site, which automates Facebook's existing search function, is intended to show Facebook users posts they may not know are public.

Level two in my privacy test was looking at data we willingly give to companies like Google. My volunteers brought their laptops and logged in. What we found provoked their most uncomfortable reactions.

On its Maps Timeline, Google is gathering a dossier about you that would make a spy jealous. Depending on how much you use Google products, there could be an hour-by-hour map of everywhere you've ever visited. Yes, everywhere. On Google's My Activity site, you can see everything else they're cataloging: searches, websites you visit in Chrome, YouTube videos you watch, even recordings of your voice to Google's Assistant.

At least Google, like a few others, presents the data in a dashboard for you to see—and delete, if you want. Half of my volunteers deleted stuff immediately. (In a coming column, I'll describe many more ways to reduce your digital footprint.)

The woman who received harassing phone calls told me she has made it her mission to scrub her name from the internet entirely. It isn't going very well. She canceled her Google and Facebook accounts, but still can't remove some info posted by others. She says several people-search sites haven't responded to her requests. "No one will hear me," she says.

Write to Geoffrey A. Fowler at geoffrey.fowler@wsj.com

Appeared in the May 25, 2017, print edition as 'You Are a Wide-Open Book on The Web.'