How to protect your data privacy: Expert provides steps you can take and explains why you can't go it alone

January 25 2024, by Nathan Schneider

Credit: Pixabay/CC0 Public Domain

Perfect safety is no more possible online than it is when driving on a crowded road with strangers or walking alone through a city at night. Like roads and cities, the internet's dangers arise from choices society has made. To enjoy the freedom of cars comes with the risk of accidents; to have the pleasures of a city full of unexpected encounters means some of those encounters can harm you. To have an open internet means people can always find ways to hurt each other.

But some highways and cities are safer than others. Together, people can make their online lives safer, too.

I'm a media scholar who researches the online world. For decades now, I have experimented on myself and my devices to explore what it might take to live a digital life on my own terms. But in the process, I've learned that my privacy cannot come from just my choices and my devices.

This is a guide for getting started, with the people around you, on the way toward a safer and healthier online life.

The threats

The dangers you face online take very different forms, and they require different kinds of responses. The kind of threat you hear about most in the news is the straightforwardly criminal sort of hackers and scammers. The perpetrators typically want to steal victims' identities or money, or both.

These attacks take advantage of varying legal and cultural norms around the world. Businesses and governments often offer to defend people from these kinds of threats, without mentioning that they can pose threats of their own.

A second kind of threat comes from businesses that lurk in the cracks of the online economy. Lax protections allow them to scoop up vast quantities of data about people and sell it to abusive advertisers, police forces and others willing to pay. Private data brokers most people have never heard of gather data from apps, transactions and more, and they sell what they learn about you without needing your approval.

A third kind of threat comes from established institutions themselves, such as the large tech companies and government agencies. These institutions promise a kind of safety if people trust them—protection from everyone but themselves, as they liberally collect your data.

Google, for instance, provides tools with high security standards, but its business model is built on selling ads based on what people do with those tools. Many people feel they have to accept this deal, because everyone around them already has.

The stakes are high. Feminist and critical race scholars have demonstrated that surveillance has long been the basis of unjust discrimination and exclusion. As African American studies scholar Ruha Benjamin puts it, online surveillance has become a "new Jim Code," excluding people from jobs, fair pricing and other opportunities based on how computers are trained to watch and categorize them.

Once again, there is no formula for safety. When you make choices about your technology, individually or collectively, you are really making choices about whom and how you trust—shifting your trust from one place to another. But those choices can make a real difference.

Phase 1: Basic data privacy hygiene

To get started with digital privacy, there are a few things you can do fairly easily on your own. First, use a password manager like Bitwarden or Proton Pass, and make all your passwords unique and complex. If you can remember a password easily, it's probably not keeping you safe. Also, enable two-factor authentication, which typically involves receiving a code in a text message, wherever you can.

As you browse the web, use a browser like Firefox or Brave with a strong commitment to privacy, and add to that a good ad blocker like uBlock Origin. Get in the habit of using a search engine like DuckDuckGo or Brave Search that doesn't profile you based on your past queries.

On your phone, download only the apps you need. It can help to wipe and reset everything periodically to make sure you keep only what you really use. Beware especially of apps that track your location and access your files. For Android users, F-Droid is an alternative app store with more privacy-preserving tools. The Consumer Reports app Permission Slip can help you manage how other apps use your data.

Phase 2: Shifting away

Next, you can start shifting your trust away from companies that make their money from surveillance. But this works best if you can get your community involved; if they are using Gmail, and you email them, Google gets your email whether you use Gmail yourself or not. Try an email provider like Proton Mail that doesn't rely on targeted ads, and see if your friends will try it, too. For mobile chat, Signal makes encrypted messages easy, but only if others are using it with you.

You can also try using privacy-preserving operating systems for your devices. GrapheneOS and /e/OS are versions of Android that avoid sending your phone's data to Google. For your computer, Pop!_OS is a friendly version of Linux. Find more ideas for shifting away at science and technology scholar Janet Vertesi's Opt-Out Project website.

Phase 3: New foundations

If you are ready to go even further, rethink how your community or workplace collaborates. In my university lab, we run our own servers to manage our tools, including Nextcloud for file sharing and Matrix for chat.

This kind of shift, however, requires a collective commitment in how organizations spend money on technology, away from big companies and toward investing in the ability to manage your tools. It can take extra work to build what I call "governable stacks"—tools that people manage and control together—but the result can be a more satisfying, empowering relationship with technology.

Protecting each other

Too often, people are told that being safe online is a job for individuals, and it is your fault if you're not doing it right. But I think this is a kind of victim blaming. In my view, the biggest source of danger online is the lack of public policy and collective power to prevent surveillance from being the basic business model for the internet.

For years, people have organized "cryptoparties" where they can come together and learn how to use privacy tools. You can also support organizations like the Electronic Frontier Foundation that advocate for privacy-protecting public policy. If people assume that privacy is just an individual responsibility, we have already lost.

Provided by The Conversation

Citation: How to protect your data privacy: Expert provides steps you can take and explains why

you can't go it alone (2024, January 25) retrieved 8 May 2024 from
https://techxplore.com/news/2024-01-privacy-expert.html