Deciding What's Private, What's Not

By Kevin B. McLachlan

The names, email addresses and phone numbers of about 50 million Uber users were stolen by hackers in 2016.[1] Last September, 143 million Equifax customers had their personal information stolen during a cyber attack.[2] Given such high-profile stories, our online privacy and security can seem under constant threat. The daily nature of being online and sharing information, the prevalence of website tracking and significant data breaches are prompting people and businesses to re-evaluate the use, sharing and storage of sensitive personal data.

Storing data is a fact of modern life, but it's worth asking how much data should you share, how should it be stored and who should have access to it? Better security is part of the solution. However, some are now advocating that companies adopt lean data practices. Such practices encourage businesses to only collect data that's absolutely needed and store it only as long as necessary. Lean data practices also encourage companies to be clear with their customers about data collection, use and disclosure.

In stark contrast, some entities see us as just another data set. Likewise for some people, sharing different pieces of information online is no big deal. Given that your online activities can be recorded by spying ads and invisible trackers and collected across all devices, services and accounts, it seems only prudent to want to know who owns your data and its intended use.

For instance, it can be analyzed, shared and sold. The new owner gets a pretty clear profile about your habits, movements, relationships, preferences, beliefs and secrets. That's information entities can exploit and capitalize upon. Your online posts, comments and details are intrinsic to the very algorithms designed to sway your sentiment about things ranging from products to politics.[3]

Various reasons may prompt concern about the collection, sharing and analysis of your online data. You may have noticed the same ads following you around on different websites. You may be concerned about identity theft. Perhaps you don't feel that companies should be allowed to make money from your personal information. Or, you don't like the thought of online searches or other information about you being recorded.

There are ways to have more control over your digital life. A good starting point: Think about what and how much you share online. Control your mobile apps to access only the information needed. Manage your profile and preference settings on social media platforms. Remember that, in many cases, free online offerings are not truly so. The price is your data.

If you want to do more to address your online presence, there are tools to help. In fact, the Mozilla Foundation, in partnership with Tactical Technology Collective, has developed something called a Data Detox to help regain control of your online digital trail. I think I'll give it a try.

> *"...prompting people and businesses to re-evaluate the use, sharing and storage of sensitive personal data."*

1. Dara Khosrowshahi, "2016 Data Security Incident," *UBERNewsroom*, November 21, 2017, www.uber.com/en-CA/newsroom/2016-data-incident.
2. Alfred NG and Steven Musil, "Equifax data breach may affect nearly half the US population," *CNET*, September 7, 2017, www.cnet.com.
3. Ramona Pringle, "'Data is the new oil': Your personal information is now the world's most valuable commodity," *cbcnews*, August 25, 2017, http://www.cbc.ca/news/technology/data-is-the-new-oil-1.4259677.