Researchers raise awareness about interconnectedness, privacy risks of online services

February 6 2019, by Bernie Degroat

Credit: CC0 Public Domain

If you are a frequent user of technology, something like this probably happens to you every day: You search the web for articles on the

nutrition needs of your new puppy and almost immediately ads from pet food companies start flooding your social accounts and web pages.

Perhaps even more mysteriously, you check the daily news and read an article about the latest science behind obesity, and the next thing you know an offer from a national weight loss company appears in front of you, even though you didn't search, share or otherwise "mark" your experience with that article.

We laugh, feel violated, maybe even get a little indignant and spout off in a social media post, but research shows many of us accept these invasions of privacy in exchange for the convenience of technology. We may even appreciate some of this targeted messaging, like a movie recommendation or the link to a cheaper source for that pair of shoes we want.

Meanwhile, companies are working to amass huge amounts of data about us, pretty much unchecked—at least for now—say researchers at the University of Michigan and Fordham Law School. The researchers, with support from AT&T, hope to help the public better understand the mechanism—so-called Application Programming Interfaces, or APIs—that allows data sharing that leaves us vulnerable to breaches like those recently making news at Facebook and Google.

Thomas Norton, executive director of Fordham Law's Center on Law and Information Policy, and Florian Schaub, assistant professor at the U-M School of Information, will present their report, "APIs and Your Privacy," at the AT&T Policy Forum's Symposium on Application Programing Interfaces and Privacy 1-3 p.m. Feb. 5 in Washington, D.C.

"It seems no day goes by without hearing about a new data breach or unexpected sharing of personal data. APIs play an important role in many of those cases as well as in our digital economy," Schaub said.

"Our goal with this report is to help consumers and policy makers understand what APIs are, what APIs companies offer and what the privacy implications of APIs are."

Norton said that in a broader sense, they hope the research "will reveal how vast the data collection business model is and how it's often difficult for consumers to detect when their information is being collected. As has been often said: when it comes to free online services, people are the product. We hope our report helps readers internalize this concept."

Application Programing Interfaces allow software programs to communicate with one another. A website may have a feature or tool its developers want to make available to other websites or applications.

In their report, the authors use the example of a kayak rental website that, for the convenience of customers, links to a weather site. An API allows the customer to know the forecast for the day when interacting with the primary site, but it also gives the weather service an idea of who is visiting the kayak rental site.

APIs allow us to view a YouTube video through Facebook, watch an ad for another computer game in order to gain more "lives" in the one we're playing, and search a company website that uses Google technology.

They are used in mobile games, search engines, social media platforms, news and shopping websites, video and music streaming services, dating apps and mobile payment systems.

"Not everyone gets the chance to see just how complex the web is—any time you visit one website, you're likely communicating with dozens of other sites, too. And those extra, invisible connections create a lot of opportunities for data collection," said Allison McDonald, a co-author of the report and U-M doctoral candidate in computer science and

engineering.

For their report and presentation, the researchers examined 11 prominent online services to demonstrate the role APIs play in gathering and distributing consumer information. These include the Candy Crush Saga mobile game, Google Search, Facebook, CNN.com, Netflix, Pandora, Amazon.com, Google Maps, the Tinder dating app, ESPN and the mobile payment app Venmo.

The researchers said a major concern is large companies like Facebook that gather so much information about people, making them "juicy targets for hackers."

"Companies should not be allowed to collect information about us without our knowledge, for reasons we don't expect and without giving us a meaningful opportunity to opt out," Norton said.

The researchers also explain the various ways APIs are used, how breaches like Cambridge Analytica can occur and how companies like Facebook have responded.

"In the 10 or so months since Cambridge Analytica, we've seen even more reports about Facebook, Google and others sharing user data in a way and at a scale that's shocking and sometimes dangerous to consumers," McDonald said. "I think this is a good indicator of how this ecosystem works and will continue to work.

"Companies will profit off of data sharing and obscure their arrangements until they're found out. The short of it: I'm unconvinced companies are tightening control on the whole. I think they're patching holes here and there when there's media attention. And that's a good reason for us to continue talking about this topic and exploring technical and policy solutions."

Schaub said consumers can do a few things to better protect themselves, ranging from considering the business model of a service they use, what might be inferred from their data and behavior, and protecting themselves with privacy browser extensions.

"It's tough to be entirely invisible on the internet because the methods of collecting data from your online habits are changing as fast as the web is," McDonald said. "But there are some things that make it harder for companies to track us and that keep us safer.

"Using an Adblocker like Adblock Plus or uBlock Origin means you'll be making fewer of those invisible connections while you browse. A 'tracker blocker' browser extension like Ghostery limits those connections, too."

Provided by University of Michigan