Worried about your Facebook data?

26 March 2018, by Shannon Nargi

Credit: Adam Glanzman/Northeastern University

Last weekend, the *New York Times* revealed that data analytics firm Cambridge Analytica misused data from as many as 50 million Facebook profiles to aid messaging tied to the Trump campaign in the 2016 presidential election.

The Federal Trade Commission has since opened an investigation into Facebook, but the entire incident has left social media users concerned about their own privacy online and how their information is being used.

We spoke with assistant professor David Choffnes—whose research includes designing solutions to internet security and privacy—to see what social media users should learn from this, and what steps they can take to keep themselves safe online.

The Cambridge Analytica case has revealed the extent to which Facebook collects and sells user data. What does this mean for the average social media user?

At this point, if you've already given Facebook information, then the horse is out of the barn and you're not going to get it back in. One of the problems with the design of the programming interface these Facebook apps use is that sometimes your own settings don't protect you. By default, when someone installs a Facebook app, it can access not only your data but all your friends' data.

It also means you've given data away not only to Facebook but probably to even more subtle sources. If you wanted to be able to share your photos from iPhoto, for example, so that you can post those photos directly to Facebook, that means that iPhoto got access to data about you, including things like employment history. Hopefully the Cambridge Analytica story can help people realize the extent to which their information is being used, and that they need to limit what is known about them online moving forward.

What are some practical steps that users can take to protect themselves?

There's a spectrum of what people can do to protect themselves. You can take it to the extreme and delete your Facebook profile and all other social media. There are a lot of people saying that's what people should do in response, but I don't think that's entirely practical. Facebook and some other platforms like Twitter are actually essential for the things we do, and at some point it's really the main way that people access vital information.

Instead, the first thing you can do is de-authorize those apps you don't need. If you participated in a personality survey like the one that Cambridge Analytica used, you probably want to turn that off and revoke access. Facebook has a settings interface that allows you to lock down information being shared and restrict apps installed by your friends that can see your own information. That's a concrete thing you can do to at least limit the data collection going forward.

Another thing to be aware of is that if you're still in Facebook and you didn't explicitly log out of the site, then anytime you visit a website that has a

Facebook 'like' button, your browser is actually communicating with Facebook to let it know that you and your specific profile, not just an anonymous person, is visiting that website. So, these privacy protections that you've set within the Facebook interface only protect you within Facebook, but it doesn't mean they're not still collecting data about you as you go elsewhere on the web.

It's important for people to realize that just trying to improve privacy in one place on the internet is generally not going to protect you from things like profile-based targeting.

Should these precautions be taken on all social media platforms, not just Facebook?

Absolutely. Everybody is focusing on Facebook right now because it's been in the news, but the way every social media platform makes money is by selling your data. It's important to be aware that most apps you use have some type of tracking software built in. Some of it can be controlled by restricting the data you make available to social network platforms, but only to the extent that the platforms have privacy settings limiting how they can share that data.

The general recommendation, though, is this: when you decide to install and use an app, think twice about whether you need the app. And, if you do use the app, think twice about the information that you provide to it. You should assume that any information you provide may be shared with other parties. Think of your online privacy like you think of any other hygiene – if you don't brush your teeth, they'll fall out. If you don't take practices to protect your privacy, your data is going to get out there.

Provided by Northeastern University

APA citation: Worried about your Facebook data? (2018, March 26) retrieved 24 June 2019 from https://phys.org/news/2018-03-facebook_1.html