Understanding Internet Privacy

Joseph T. Parsons

dq3685ct@metrostate.edu

I just so happen to be old enough that I missed out on middle-school lectures about social media safety. While Facebook was quite big when I entered high school, adults had not quite caught up with the technology. Schools were more focused on stranger danger (scary chat rooms!) than they were on the actual threats of my time, like cyberbullying and revealing too much information on social media.

This has changed. I expect most college freshmen and sophomores probably did get those lectures, and in any case older students have had *plenty* of time to learn about social media safety. I’m not going to reprise those lessons here, but I would like to take a look at some of the lesser-known privacy losses people encounter on the internet, and how to avoid them.

(I would also recommend checking out my previous article on Windows 10 privacy, available at **themetropolitan.metrostate.edu/issue/2016/09/002/**)

**Facebook Knows Which Websites You Visit**

No, really. Facebook knows a lot about which sites you visit. Any website that includes an un-customized Facebook “like” button, or page widget or comment feed is a website that Facebook knows you’ve visited. Some websites don’t include any of these, but instead include “Facebook pixel” in order to track the demographics of their users—which is done by aggregating the Facebook profiles of people who visit those websites. Those websites won’t know exactly *who* is using them, but Facebook will know everybody who is using those websites. (Disclosure: The Metropolitan online includes the Facebook “Like” button, enabling tracking. The main Metropolitan State website includes Facebook pixel.)

Now, in general, this applies to other large media platforms as well, like Google. Google does, for instance, have the ability to connect ad hits on any webpage with a distinct user account. Even if you tell Google not to use personalized ads, the company still has the capability of connecting every ad you view with your Google account. Where Facebook seems to differ is that they do this quite intentionally. Google doesn’t *need* account information to show an ad, and if you disable tracking, they almost certainly discard the information immediately. Facebook offers no equivalent—if you are logged into your Facebook account, they will know what pages you visit. That’s the point of the pixel tracking, after all: to leverage your profile information as demographic information.

Now, there is a sure-fire option to “opt out” of this type of tracking: AdBlock. There are many AdBlock extensions available, AdBlock Plus (adblockplus.org) and uBlock Origin (available on the Chrome Web Store) being two good choices. Both will automatically block *most* tracking, ads included, and can be easily configured to block all social media trackers. (For AdBlock Plus, social media blocking can be enabled by adding “Fanboy’s Social Blocking List” from easylist.to; on uBlock Origin, you can enable this list directly from the settings menu under “3rd-Party Filters.”)

**Google Knows Where You Were Last Summer**

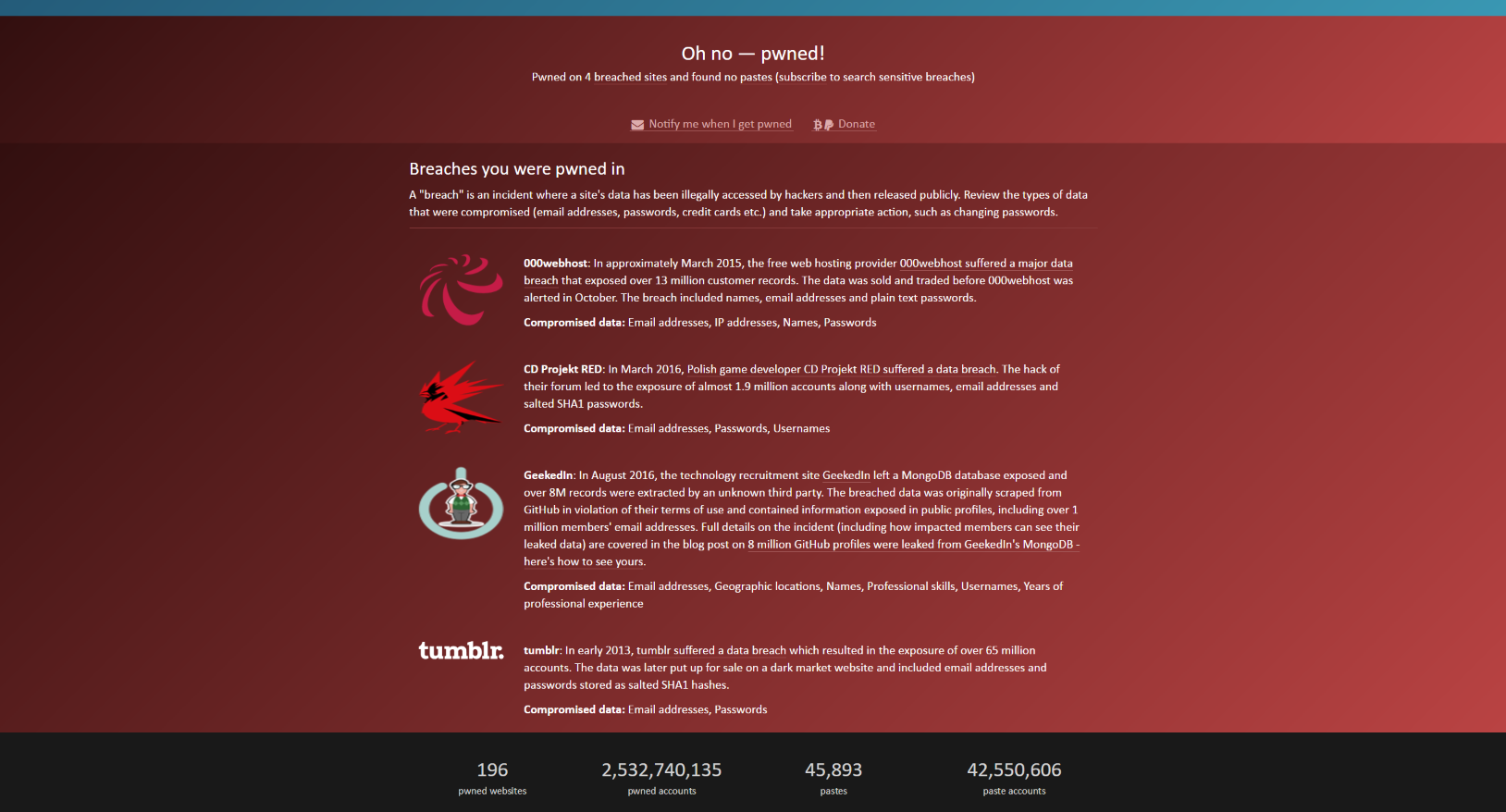
I actually find this feature quite cool, but most people don’t seem to know about it: Google keeps a log of the places you visit. Whenever you use GPS through a Google service (be it on Android or iOS), Google keeps a log of it. It uses this information in some very useful ways. For instance, Google Now may use it to remind you where you parked, and Google Maps uses it to ask people to provide reviews for restaurants they’ve visited.

Still, Google is remarkably transparent about this information. You can view everything they know at **google.com/maps/timeline** in an easy-to-use day-by-day map of your activities. You can also disable your location history completely by going to **myaccount.google.com/activitycontrols/location**. But, honestly, I prefer to keep mine on because it’s nice having an automatic log of my activities.

**Password Leaks Can Open Up All Your Accounts**

One persistent issue with keeping your data private is keeping the accounts holding your data private. Everybody should be using a password manager (I highly recommend reading [themetropolitan.metrostate.edu/issue/2016/03/002/](http://themetropolitan.metrostate.edu/issue/2016/03/002/) for more on that). This ensures the use of only random, varying passwords for every site, but in practice most people just reuse the same two or three passwords for every account. And, unfortunately, websites are often less secure than we realize, with prominent website hacks releasing onto the internet millions of user passwords every year.

If you’re the reactive (instead of proactive) type, and don’t use a password manager, you can at least check haveibeenpwned.com to see if any accounts associated with your email address or password have been leaked. If you see that they have, **make sure you change the passwords to any accounts that reused compromised passwords**!



Caption: In total, my five-year-old email address is associated with four (4) different breaches, three of which contain passwords! (from haveibeenpwned.com)