CARLTON FIELDS

Your Apps May Be Selling You Out

CYBERSECURITY AND PRIVACY | TECHNOLOGY | TECHNOLOGY & TELECOMMUNICATIONS | TELECOMMUNICATIONS | JULY 12, 2017

Amy E. Furness

While most people are vaguely aware, even if they are in denial, that their browsers give advertisers access to their search histories, they are probably unaware that information is being sold or given to third parties via the apps they use on their personal phones or mobile devices.

Nothing in Life Is Free

If you have ever downloaded a “free” app, you may have pondered how the app’s creator can maintain a financially viable company by giving away its product. The answer soon becomes evident when an advertisement pops up, interrupting your interaction with the app. The less obvious answer may come to you when you uncomfortably wonder how the ad that just popped up somehow relates to the items you browsed on Amazon a few days ago. Coincidence? Probably not. This happens because, in addition to selling advertisements, app creators may also access and sell information collected from your phone to allow advertisers to customize the ads they send to your device.

Each app you download to your phone is designed to interact with you in different ways. Often this means it will also interact with and access various forms of information on your phone. For example, you probably give social media apps access to your contacts to expedite the process of creating a list of “friends” or “followers.” You may also give the apps access to your camera and photos in order to take and post photos on the app. In addition, if you want your posted picture to automatically include your location, you must provide the app with access to your location services. All of this information has value to third parties who want to send the most targeted advertisements possible to increase the chances that their products will appeal to the individuals targeted.

So, there is a lot of money to be made by creating an app that accesses personal information and allows the creator to monetize it. Most people probably assume the access they give an app or the personal information they input in an app on their phone is strictly confined to their personal phone. However, it is important to be aware that this assumption is incorrect and could potentially lead to a significant loss of privacy or even identity theft.

Et Tu, My Favorite App?

In April 2017, the news broke that the app Unroll.me sold information regarding users’ rides on Lyft to competitor Uber. Unroll.me allows users to organize and delete unwanted subscription emails. As such, it requires access to users’ emails. Unbeknownst to its users, the app combed through their emails for Lyft ride receipts, anonymized the data, and sold it to Uber. With this information, Uber tried to gain a competitive advantage over Lyft. The app’s privacy policy did state that it might collect and sell nonpersonal information for any purpose. Still, users were upset to learn it was happening.

While it is apparent that using an app like Unroll.me requires providing access to your email, other apps access your email even though such access appears unnecessary to use the app adequately. They may also access your contacts, text messages, call history, social media accounts and browser history.

Personal data downloaded by apps is frequently sold to advertisers. Even when the original developer never distributed personal data, if the app is sold, all of the information it has collected is sold along with it. Personal data in the hands of an app is also susceptible to theft. Once personal data is purchased or stolen, it increases your risk of identity theft. For example, personal data could lead a cyberthief to the answers to your personal security questions.

This is how it plays out: You are a member of your elementary school alumni Facebook group. A hacker obtains information

drawn from your Facebook account and now knows the answer to the security question, “what elementary school did you attend?” or “where was your elementary school located?” In this manner, the personal data obtained and transmitted by your apps is not just a matter of privacy, but also a matter of cybersecurity.

Breaking Down the Data Collected by Some of the Most Popular Apps

Facebook’s policies notify users that Facebook owns all information gained from their use. This not only includes the pictures you upload or information you post in a status update. Facebook retains the right to collect information regarding your searches, the friend requests you accept and decline, and even the messages you exchange through its messenger service. Facebook also tracks the sites you visit if they include a Facebook “like” button and information regarding the devices you use to access the app. Facebook reserves the right to keep all of your information, even after you delete your account.

Health-related apps track things such as a user’s calorie intake and exercise level when the user inputs what he/she ate throughout the day and the amount of exercise he/she did. Accordingly, the information available to the app depends on the amount of information the user inputs.

Music streaming apps may collect and potentially sell information regarding music choices, and users’ age and gender. When an advertiser learns a user’s music choices and basic demographics, it can more easily figure out what the user might be interested in and then send the app ads specifically designed to entice that user. Musical choices are highly personal, similar to reading choices, and it is rather unsettling to know that third parties know what you are listening to in the privacy of your home or car, or through your headphones.

Perhaps, “There Ought to be a Law”

Recently, an app user took his complaint regarding the sale of his personal information to federal court. Kyle Zak sued the Bose Corporation on behalf of a purported class of individuals due to Bose’s collection and transfer of information regarding their music choices through the Bose Connect app.

In the realm of technology, the law is woefully behind the times. Lawyers and judges struggle to fit a round peg into a square hole. In Zak v. Bose, the plaintiff argues that Bose is violating the Federal Wiretap Act, which prohibits the intentional interception of electronic communications and their intentional disclosure. However, this is a criminal statute first codified in 1968, almost 50 years ago. Similarly, the plaintiff alleges violation of the Illinois Eavesdropping Statute, a state criminal statute, originally drafted in 1961. Even subsequent amendments to these statutes have not been made with an eye toward encompassing today’s technology or the circumstances underlying cases like Bose. These laws, or similar state iterations, have not yet been tested in the context of an app.

Rather, the landmark cases regarding privacy in the context of individual use of technology stem from website and browser use. In Perkins v. LinkedIn, 53 F.Supp. 3d 1190 (N.D. Cal. 2014), users sued LinkedIn because it harvested their contacts’ email addresses and sent multiple emails inviting them to join LinkedIn. In response to LinkedIn’s motion to dismiss, the court first analyzed LinkedIn’s argument that plaintiffs lacked standing because they could not show an injury due to LinkedIn’s conduct. The court disagreed and held there was value in plaintiffs’ identities, which plaintiffs claimed were being improperly used to portray their endorsement of LinkedIn without their consent. However, the court dismissed plaintiff’s claim that LinkedIn violated the Wiretap Act by obtaining their contacts’ email addresses. The court found that plaintiffs consented to the alleged interception of their contacts’ information by agreeing to various permissions the site requested.

Similarly, in In re Google Inc. Cookie Placement Consumer Privacy Litigation, 806 F.3d 125 (3d Cir. 2015), the plaintiffs attempted to use the Wiretap Act to obtain damages from Google and others who allowed cookies to be placed on their browsers to track their internet use for advertising purposes. On review of an order granting defendants’ motion to dismiss, once again, the court began with an analysis of the standing issue. The court found that plaintiffs did have standing even if they could not show a monetary loss due to defendants’ conduct. Regarding plaintiffs’ Wiretap Act claim, the court held that the URLs for the site plaintiffs visited could be considered “content” under the Act because they could be highly detailed, revealing very specific information regarding the sites and information obtained. However, the court found plaintiffs did not state a claim under the Wiretap Act because defendants were the intended recipients of the communications with plaintiffs. The Wiretap Act only protects the interception of electronic communications by someone who is not a party to the communication. Because defendants obtained information from plaintiffs when plaintiffs entered search terms in the browser or visited sites after cookies were placed on their browsers, the court reasoned that the advertisers were parties to the communications. The court held that even though plaintiffs claimed they did not intentionally communicate with the

advertisers because they were allegedly unaware that the browsers were allowing the advertisers to participate in the communications, the advertisers were still the intended recipients of the communication.

Nowadays, most apps bury within their privacy policies language that allows them to collect, transfer and/or sell information collected with the user's permission. These warnings are likely sufficient to protect the apps from most individual causes of action that could potentially be asserted.

Protecting Privacy

While it is disconcerting to learn that your personal information and preferences may be sold or stolen, you always have the option to forgo providing apps with access to your personal information, or downloading any apps at all. The most popular app stores require the apps they sell to ask permission to do things such as obtaining users' locations or access to cameras. If you deny the apps these permissions, your personal information should be safe from their grasps. However, your interface with the app will suffer accordingly. Imagine trying to use a map app that cannot access your location.

You may review the permissions you have granted each app in the settings of the app and your phone's operating system. You should also use caution when signing up for apps through Facebook and Google. While it may save you some time and effort to avoid creating a new user name and password, when you log on to a new app through Facebook or Google, you grant those apps permission to access the information you post on Facebook or the searches you conduct on Google. Such information may include a list of your contacts, your pictures and your status updates. To disassociate an app from Google, visit the Google security page and go to "connected apps & sites" and click on "manage apps." Similarly, in Facebook settings, clicking on "apps" allows you to click on an "x" next to any app you would like to disconnect from Facebook.

Deleting an app should protect you from further collection and dissemination of information. Apple prohibits app developers from tracking users after their apps are deleted. However, some apps can "tag" a phone, which places an identification on the phone. Later, it can be determined that the app was once on that phone. Similarly, phones can be tagged with the last Wi-Fi network they were logged into.

Finally, for additional peace of mind, security and privacy apps can be downloaded that will scan the apps on your phone to determine which ones send your personal information beyond your phone.

In sum, we should all be aware that our phones and personal devices are not impenetrable private boxes if we decide to download and use apps. Be aware of the permissions you give apps to access your information and always proceed with caution.