CONSUMER NEWS
SAN DIEGO CITY ATTORNEY'S OFFICE

Mobile Apps and Privacy: How to Keep Yourself Protected

March 2014

Mobile Applications (Apps) can be functional, entertaining, and useful. However, they can also be deceiving. Personal information about the apps user, including phone & email contacts, photos, geolocation, and internet history, can be stored, used, and even sold to third party marketers. Privacy concerns and technological vulnerabilities are increasing rapidly. Often users do not know that their personal data has even been accessed or distributed.

To protect one's privacy, it is essential to know *what* information is made available to App developers and *how* it is being used. New laws are emerging to regulate fair disclosures to consumers; however there is no complete shield available to consenting app users.

HOW DO MOBILE APPS WORK?

Apps are software programs downloaded into smartphones, tablets, or other mobile devices. Apps are available to consumers through online stores and through specific operating systems, sometimes even at no cost. Apps perform a wide variety of functions including mobile banking, calendaring, mobile directions, games, news, and social media. Once an app is downloaded into your mobile device, users may be asked to give authorization to the app to gather the informational content or geolocation. Users may also be asked to consent to privacy policies.

WHY YOU SHOULD BE CONCERNED

ID theft is a prevalent problem in our technology saturated world. Smartphone, tablet, and other mobile device users are subject to risk. Disclosures are often disregarded and often contain consent to access personal information. Anytime personal information is exposed, a threat of ID theft exists. Specifically, with mobile apps, the mobile software programs integrate into the mobile device's core operating system to access information that may be used or distributed, contrary to the app's function.

Smartphones and mobile apps are also vulnerable to malware and viruses, just like computers. Once installed, these malicious software programs secretly track the phone's use to gain personal information. Hackers then may use the personal information to commit financial fraud and ID theft. For more information about ID theft, refer to www.idtheftcenter.org.

RECENT PRIVACY BREACHES

On February 21, 2014, Apple released a security update indicating that hackers, finding a code flaw, may be able to capture or modify data of some iphone, ipod, and ipad users. What this means is that hackers could intercept interaction with a trusted site, such as mobile banking or email, retrieving personal information, including credit card information, passwords, and geolocation.

In January 2014, a researcher exposed a security flaw in Starbucks' app, exposing user geolocation and password information. Starbucks responded to the report by conceding the flaw existed, but stated that no privacy breaches had been reported. Starbucks issued an online letter to customers, offering an updated version of the app which was developed to provide additional protection.

In another case, 4.6 million users of the app Snapchat (a photo and video sharing app) were vulnerable to user name and email address exposure. This incident was followed by a recent spam hacking, the smoothie hack, in February 2014. In the first hacking, the information was publically released for download to an online database. Those behind the database claimed they posted the database to raise public awareness to privacy exploitation and to incentivize Snapchat to increase security measures.

Users of the mobile dating app, Tinder, were also subject to exposure. Researchers determined that a flaw in the geolocation server exposed precise locations of users, within 100 feet of a user's whereabouts. The flaw was exposed for months without being publically addressed. The flaw would have permitted stalkers to locate their victims, using the apps geolocation device.

WHAT YOU NEED TO KNOW:

- **Privacy Policies.** Privacy Policies are not the same as security settings. General security settings do not automatically protect your privacy. App users may need to manually set privacy settings for each individual app. An app's actual privacy policy statement may not always be provided upon installation. Privacy policies subsequent updates may also not be explicitly provided.

- **Geotagging.** Geotagging is a feature that allows your phone or app to pinpoint your location and connect that location to photos, video, and text messages. Enabling geotagging permits mobile device users to voluntarily disclose the precise location of where a photo was taken or a status was made. Increasingly, criminals are taking advantage of this voluntarily disclosed information by targeting individuals that are away from their homes and burglarizing them.

In a consumer context, geotagging, also known as geolocation, has been increasingly used to do target marketing. Sensors, installed in businesses, are tracking consumer's whereabouts and then using that information to send target marketing advertisements. Your next trip to get frozen yogurt may activate a coupon to be sent directly to your phone. Disabling geolocation will prevent personal surveillance.

There are not any regulations against target marketing for adult consumers, however the Children's Online Privacy Protection Act restricts target marketing and the collection of personal information of children under the age of 13.

- **Marketing and Data Brokers.** Information taken from the use of mobile devices can be collected and distributed to third parties. Currently, only children are protected against the sale of personal information data brokers.

HOW TO PROTECT YOURSELF:

(1) Check the legitimacy of the app. One key recommendation is checking the source of the app you are using. Hackers may create fake apps to collect personal information, deceiving consumers by using familiar looking logos or features. For example, a hacker may develop a fake online banking app that would then collect personal financial information. One way to check the legitimacy of the app is to read reviews by previous app users.

(2) Read the privacy policies and permissions. Often mobile device users do not know what information is actually being released through the app. Often this information is contradictory to the apps purpose and that information is being sold and distributed to third party marketers. By reading privacy policies and permissions, mobile device users can protect themselves against the distribution of information. Even with legitimate apps, private information may be insecure.

(3) If information is being collected, know how it is being used. For example, determine whether it is really necessary that an online gaming app have access to all your email contacts.

(4) Be cautious about apps children download. If children have access to the mobile device, monitor what has been downloaded and the privacy settings associated with the app.

(5) Be cautious about using public wifi. Always remember that use of public wifi is vulnerable to hackers.

(6) Consider Anti-Virus software. There is antivirus software available in the market, even for phones.

(7) Consider using a backup program. Backup programs may allow remote ability to wipe out a mobile device's data, in the event the mobile device is stolen or lost.

For more information about keeping yourself protected, visit www.onguardonline.gov.

WHAT TO DO IF YOU THINK YOU ARE A VICTIM:

✓ Check your credit report for any suspicious activity. The website www.annualcreditreport.com, authorized by federal law, offers all three credit reports, for free. Be cautious of using other credit reporting agencies.

San Diego
City Attorney's Office
Consumer and Environmental Protection Unit
(619) 533-5600

Newsletter written by
Shannon A. Wicks, Legal Intern.

The information provided in this newsletter is intended to convey general information and is not intended to be relied upon as legal advice.

To report violations of consumer protection laws, call the City Attorney's Hotline at **(619) 533-5600.**