Published on *The National Law Review* https://natlawreview.com

Security Risks: Smartphone Apps and Sensitive Data

Article By:

Bruce H. Raymond

As discussed in an earlier post, the release of ***Pokemon Go*** raised speculation about app security failures, including reports that the app's standard permissions released user's ***Google*** data and emails to the game's developers. While investigation did not reveal Pokemon Go to be more dangerous than other apps, it would be foolish to end the conversation about app security on that sigh of relief. Mobile Apps do not come without security risks to individuals, businesses, or even governments, and risks vary widely on different platforms and between different apps. If an employee's smartphone contains sensitive company data alongside gaming or productivity apps, there are very real risks to be aware of when trying to prevent security breaches.

Smartphone apps: what are the risks?

Most smartphone apps are not primarily out to steal data, just to make a profit. That objective can be accomplished through direct advertising within the app, such as banner ads, or through the sale of consumer data obtained through the app to other advertisers. Many apps use a hybrid of these two approaches, with the app targeting advertising based on the information it knows about the user from the data is it granted access to. Targeted advertising, while perhaps intrusive or distasteful to individuals, may not present much of a threat to your business. What this type of advertising does signal, however, is that a large quantity of data is being collected and stored by developers. Once that data is out in the world, the security protocols in place to protect it are out of your control. If sensitive data is collected by a mobile app, there is a risk that that data will get into the wrong hands, either because it is stored on an insecure server or transferred in an unsafe manner. In a world where sensitive business data can live alongside third-party apps in every employee's pocket, the risks associated with these apps multiplies.

In addition to concerns related to unsafe data collection methods, it is also possible that the app itself could be compromised. In July, CBS reported the following risks in conjunction with smartphone apps:

- Malware or spyware: one investigation showed that between 75 - 97% of Apple and Android apps were breached

- Stolen financial information, including credit card data and checking account information

- Access to smartphone cameras and microphones being used to transmit audio and visual data. One flashlight app even went as far as to access the microphone on users' phones, then transmit an encrypted data stream to a server in Beijing

- Collection of data, including call logs, text messages, photos, and contacts

Mobile apps have the potential to be a powerful tool for hackers, and while companies like Apple and Google have an economic incentive to keep their app stores as safe and free from these risks as possible, they cannot eliminate all risk.

Minimizing Risk

Fortunately, the risks associated with smartphone apps are not unavoidable, and conscientious security policies can go far to prevent security breaches. Employees using smartphone apps for entertainment and relaxation to supplement the business uses of the device may be unaware of the risks associated with these apps, however, so developing and enforcing policies to prevent breaches is of the utmost importance. In developing app policies for employee smartphone use, some recommendations from industry experts include:

- Only downloading games and apps from official stores, such as Apple or Google Play. Third party stores are more likely to have fake, risky versions of popular apps that contain malware.

- Forbidding "jailbreaking" or "rooting," which are often completed intentionally by users to allow them administrative access to the device, but disable security protections and open devices up to attack

- Giving apps permission to access only data that is needed for the app's operation

- Keeping the app updated to the latest version, where security issues may be more likely to have been fixed. Similarly, requiring that platforms and operating systems be kept updated.

- Deleting any unused or unnecessary apps to minimize risk

Staying ahead of new technology and developing proactive policies to avoid a security breach will help keep your business' and clients' data safe.

National Law Review, Volume VI, Number 228

Source URL:https://natlawreview.com/article/security-risks-smartphone-apps-and-sensitive-data