REPRINTED FROM

App DEVELOPER Magazine

March 2014

Should Mobile App Developers Create Analytics to Track the NSA?

BY ADAM D.H. GRANT

Before you read on, do not think that this article is political in nature or advocates anything remotely approaching what the title suggests. Contrary to the “hook” contained in the title, the purpose of the article is to educate Mobile App Developers on what is reportedly done to the information obtained by the apps they develop.

During this past year, the news about just how much privacy do the consumers have, want, think they want or hope they still have, has been endless. During this past year, Edward Snowden (the former National Security Agency contractor) shed light on just how much information is being gathered and by whom. The consumers also learned that the mobile app, “Angry Birds,” and others, gather far more information than they ever dreamed about.

As I speak at Mobile App Developer Conferences across the country, I am frequently asked about consumers’ expectations and what can be done to address these issues. As a result of mobile apps that are “free to play” or “advertising supported” a great deal of information is obtained from consumer when they use the apps. As part of the emerging mobile technology, with each new smart phone developers have the opportunity to obtain even greater amounts of personal data and share that data over endless networks. According to numerous previously undisclosed documents, some of the most valuable unintended intelligence tools are the so called leaky apps that effusively share identification codes to geolocation information.

Prior media leaks illuminated NSA’s propensity to shuffle through phone records, texts, online games and internet traffic. The app’s program analytics allow the program to eavesdrop on information that identifies a user’s age, location, address list and other detailed parts of their lives. As one who represents Mobile App Developers, I encourage the use of these analytics. The analytics help improve the products by teaching the developers how users interact with the product. According to the documents provided by Snowden, the NSA has been working on how to collect and store data from smartphone apps as early as 2007. This past year’s news stories described the spying on mobile networks, but recent documents shared by The New York Times, and other publications, provide a much higher level of insight into what is collected from smartphones and mobile apps. According to certain British documents, the effort was part of an initiative called “the mobile surge.” In the document, a NSA analyst enthusiastically declared the information was “golden nugget.”

The documents arguably show that the NSA routinely obtained the information from apps, and in particular from apps on smartphones. Newer apps, according to certain documents, are culled by the NSA. So, why is all this information about what the NSA is allegedly doing with the information obtained from leaky apps important to you, the Mobile App Developer?

The information contained in this article is important to the Mobile App Developer for two important reasons; First, it should guide the developer as to what should be disclosed to the consumer. Second, it should encourage the developer to how this disclosure should be made to the consumer.

At its core, a developer needs to provide concise information on how the data is used and whether it is sold to third parties. If the developer transmits the personal identifiable information to services in ways that are easily eavesdropped, then the developer should revisit the app’s security protocols. The app should allow the consumer to say, “no more” or “yes” to this type of data, but “no” to some other data. A consumer may allow an app to follow them as they drive through their everyday lives, but not allow access to their contacts or photos. Choice and ease of choice is something that must be part of the app. Additionally, if a consumer declines access to some information, it should not adversely affect the apps functionality. At its heart, such a concept means that the developer should collect only the necessary data for the app. A translating app really does not need access to a consumer’s photographs to improve its functionality.

How the disclosure is made becomes an important part of the app and consumer interface. “Privacy by Design” has been the FTC’s mantra for the past two years. Layering the privacy notices so that they are “just in time” is another means of making sure that consumers are provided with the options, but only when the options are necessary. If the app needs information only at a certain time, or in a certain window, then there is no need to collect the information unless the consumer reaches that point in the app.

The endless number of apps that hit the market on a regular basis and the lessons learned from reading the NSA documents released by Snowden are two pieces of information that when put together lead to one conclusion; App Developers must be mindful of what information is taken and address the consumer’s concerns about their privacy. By providing clear and timely notices the developer will be proactively address the consumer’s concerns – and hopefully download more of your apps!