Fairfield County Business Journal

Westchester Business Journal

Mobile Insecurity: Part 1

By Bruce Newman

January 24, 2013

Mobile application insecurity, the secretive acquisition of information from your mobile phone, is a growing problem most mobile users are unaware of. With smartphone sales expected to surpass personal computer sales for the first time later this year, it has the potential to be an area of increasing concern and conflict.

The majority of information collected by mobile applications (apps) primarily consists of geographic (geo) location, email information and phone ID. Other pieces of information, including user preferences, calendars and photographs are also regularly captured. This data is collected and sold to various advertising and third-party companies for use in advertising and marketing campaigns.

Geolocation is particularly useful since it can result in relevant ads that are proximate to a person's location. An example of this power is the appearance of a mobile ad for a store special when the user gets within 200 yards of that store. Additional information including personal preferences can refine the targeted audience.

According to a 2013 eMarketer study, the $13.63 billion amount of mobile business (7 percent of total retail business) is expected to increase to $38.4 billion, or 15 percent of retail in 2013.

With this emerging mobile market and technology designed for location and context-sensitive advertising, there's substantial reason why advertising firms are viewing this mobile realm as extremely potent and lucrative. Mobile banner advertising alone is expected to exceed $1.2 billion by 2014.

Yet, much of this comes down to a matter of privacy. Do mobile users really want to have their geolocation — and other information — transmitted from their phone without their approval?

According to a recent New York Times article, Angry Birds, the popular mobile game with over 1 billion downloads, "possesses a ravenous ability to collect personal information on its users." Many additional and seemingly innocuous games and apps — even including a Bible app — are even more intrusive, downloading calendars, pictures and contact lists.

To put it in perspective, think about it this way. There are more than 600,000 apps currently available, with more being produced every day. The majority of these apps are free. How are these developers making money if they are giving away their apps? Yes, they can possibly generate new business from their app or maybe accept advertising. But another way of

generating revenue is through the surreptitious collection and sale of personal and geo-information.

Since the Federal Trade Commission (FTC) requires a disclaimer for each app, to better understand its role and the limitations and implications of a disclaimer, I spoke with Chris Librandi, an attorney with law firm Levett Rockwood P.C. in Westport. According to Librandi, who has significant experience with digital security issues, the FTC has jurisdiction in this area of mobile security and the right to impose fines on offending companies.

Not surprisingly, the only significant legal protection against mobile information theft is when it involves children below the age of 13. In this instance, any app that collects data and is targeted towards children requires the signed consent of a parent or legal guardian before it can be installed. (If the app does not collect data, it does not require signed consent.) I can understand this for a SpongeBob SquarePants app, for example, but what about an app like Angry Birds that children also enjoy but is directed toward adults?

Librandi said it's in the company's best interest to create a disclosure policy that meets FTC approval, particularly when children are involved. It seems that the FTC has the ability to level a fine of $11,000 for each installation of an app. For an app like Angry Birds, this could result in a fine in the millions of dollars. Unfortunately, many children's apps do not follow even this simple requirement.

In a December 2012 FTC report that I will discuss in Part 2 of this column, a Pew study reported that 54 percent of adults did not download an app once they became aware "of how much personal information it would collect."

Part 2 of this column will continue a discussion of these issues and include additional legal insights from Librandi.

Bruce Newman is the president of wwWebevents.com, a division of The Productivity Institute L.L.C. in Carmel, N.Y. He is a social media guru and a specialist on webinar creation and promotion. Newman is currently completing a comprehensive webinar training course, The Complete Webinar Training Course —Everything you need to know to create and promote highly successful webinars, which will soon be available. He can be reached at bnewman@prodinst.com.