

Feb. 4, 2013

## **An app-etite for data-gathering**

By Bruce Newman

*This is the second of two columns. The first appeared in last week's edition*

If a mobile app does not collect any information from a mobile device, no disclosure policy is required.

However, once any information is collected, the Federal Trade Commission (FTC) requires the presence of a disclosure document. For children under 13 years old, this disclosure document requires the signature of a parent or legal guardian. This is in accordance with the FTC's enforcement of COPPA (Children's Online Privacy Protection Act). For 13-year-olds and older, no signature is required. However, a disclosure policy is still required.

In many cases this information in question consists of geodata, email information and phone ID, although it can extend far beyond this to include calendars and pictures. According to Chris Librandi, an attorney with the law firm Levett Rockwood P.C. in Westport, whose practice includes digital security matters, the FTC looks very differently at companies with a weak disclosure policy versus one without any policy. To avoid any difficulties with the FTC and watchdog groups, the disclosure should list all the different types of information that are being collected. However, for various reasons – including ignorance of the law and it being bad for business, the majority of companies collecting data do not have any disclosure policy.

Most adults consider this surreptitious acquisition of information to be extremely intrusive. According to a July 2012 report on mobile phones and privacy, “78 percent of the U.S. consumers surveyed considered the information on their mobile phones at least as private as that on their home computers.” Furthermore, “92 percent of the respondents said that they would ‘definitely’ or ‘probably’ not allow the use of their locations to be used to tailor advertising for them.” A Pew study reported that 54 percent of the respondents refused to download an app because of its data acquisition capabilities.

Interestingly, these findings are in sharp contrast with the excitement being expressed by advertisers and marketers concerning the “new frontier” of mobile advertising. According to a mobileSquared study, “70 to 80 percent of brands that are active in mobile are now inquiring about how they can capitalize on the location element that mobile delivers.”

Thrust into the middle of this argument is the consumer and the FTC.

It is the FTC's responsibility to monitor the disclosure policies of every app that collects data. However, with more than 600,000 apps currently available and increasing daily in number, it is an overwhelming task for the FTC's 2,500 investigators to examine all of the apps that collect data. According to Librandi, the current state of the FTC is reactionary. It is largely dependent on

whistleblowers, people and watchdog groups that test the apps and then notify the FTC that there is a potential problem. Even then, change can happen slowly.

Following a yearlong investigation, the FTC discovered that 60 percent of the apps they studied were transmitting information acquired on their mobile device to the developers, analytics companies, ad networks or some other third party. Only 20 percent of the apps had a disclosure policy.

The obvious solution is to require every app developer that captures information to have a disclosure policy detailing what data they are transferring. Laws may be changed to require this level of detail. However, since this flies in the face of Internet marketing, it is subject to considerable pushback from such powerhouses as Apple and Google which are very protective about this potentially highly lucrative revenue stream despite direct negotiations with the FTC. Without an industrywide agreement, the FTC – with limited power and resources – can only focus on individual companies with the most common result being a requirement that the app manufacturer have some type of disclosure policy even if it is misleading or insufficient.

Will most app manufacturers include a detailed disclosure policy? It's doubtful, particularly since it can cost them business. Instead, they either ignore the disclosure requirement, claim ignorance or merely copy an existing nonspecific disclosure document.

Are there apps that can block such companies as Apple from tracking you? Yes, there are a few including one called Jailbait, but Apple may void your warranty if you load it.

Since the FTC does have the power to level some considerable fines, it does have some clout and is forcing the industry to accept some changes in their policy. It has also had some successes including forcing Viacom to pull its SpongeBob app that was directed at children while surreptitiously acquiring and transmitting email addresses.

After all of this discussion, the relevant question to ask as a consumer is, "How do I know if my app is transmitting my information (which I consider confidential)?" And right now, unfortunately, the answer is that you don't. One action you can take is to Google the app and check its disclosure policy (if one exists). You should also seriously consider clearing your browsing history and turning off your geo locator.

Mobile computing is rapidly becoming a major part of our everyday existence including how we make purchases and do business. It is very important that people realize that issues of security and privacy – mobile insecurity, are a major byproduct of this rapidly evolving technology.

*Bruce Newman is the president of wwWebevents.com, a division of The Productivity Institute L.L.C. in Carmel. 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.*