The Apps Act of 2013

By Adam D.H. Grant, JD

WHAT EVERY APP DEVELOPER SHOULD KNOW

In January 2013, the California Attorney General issued a report entitled, *Privacy on the Go; Recommendations for the Mobile Ecosystem*. In the very next month, the Federal Trade Commission issued its own report, *Mobile Privacy Disclosures; Building Trust Through Transparency*.

Finally, Congress is talking about the country's concerns over privacy and is considering new legislation directly impacting mobile app developers. On May 9, 2013 Rep. Hank Johnson introduced *The Application Privacy, Protection, and Security Act of 2013*. According to Rep. Johnson's summary, "The APPS Act would require that app developers maintain privacy policies, obtain consent from consumers before collecting data, and securely maintain the data they collect."

The purpose of this article is to unlock the meaning behind the legalese and tell all mobile app developers what they need to know.

DOES THE APPS ACT APPLY TO YOU?

Does this law apply to every mobile app? No. It only applies to mobile apps that collect personal data about a user. If your mobile app does not collect personal data, you can stop reading this article and find something else to amuse you for the next few minutes. On the other hand, as virtually every mobile app collects some form of personal data, reading the rest of this article is likely a better idea.

So the real question is: What is the definition of "personal data" according to the APPS Act. A simple question, but the problem is, at least at this point, the answer is not so simple. According to the APPS Act, personal data "shall have the meaning given such term by the Commission (the Federal Trade Commission) by regulation, except that term shall not include de-identified data."

So what type of "finger print" does the FTC currently think is personal data? There are a number of sources to look at for that information. In February 2013, the FTC issued a report entitled, *Mobile Privacy Disclosures; Building Trust Through Transparency*, http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf. In the report, the FTC discusses the efforts of the National Telecommunication and Information Administration (NTIA) to develop a code of conduct, which will assist in mobile application transparency. The FTC report states, "to the extent that strong privacy codes are developed, the FTC will view adherence to such codes favorably in connection with its law enforcement work." In other words, if a mobile app developer complies with the code of conduct, the FTC might not prosecute.

As of April 2, 2013, the code of conduct requires a privacy notice

when an app collects the following types of data: biometrics (info about your body, including fingerprints, facial recognition, signatures and/or voice print), browser history, text log, contacts (including social networking connections), financial information, health/medical/therapy information, location or user files (files stored on the device that contain your content). So, "What is personal data?" According to the FTC, the answer appears to be…. everything about a person.

If personal data is virtually everything, then what does the FTC think is "de-identified data?" Why is this important? Because, if an app collects information that can't reasonably be used to identify or infer information about a particular person or mobile device, then no privacy notice is required! Of course, the APPS Act uses vague words like, "can't reasonably be used to identify," or "reasonable level of justified confidence," which do not engender much confidence with anyone when they are trying to determine whether they are complying or not with a Federal law.

Privacy law as it applies to health information allows for two methods to identify whether you are dealing with de-identified data. First, you can have an expert give you an opinion that the data has been "de-identified." Second, which is called the "safe harbor," requires that the developer remove all kinds of personal identifiers, like addresses, names and zip codes from the personal data. Of course, if you "de-identify" the information, then it becomes less valuable to the apps owner.

WHAT DOES THE APPS ACT REQUIRE?

The APPS Act requires the mobile app developer to develop a privacy notice which tells the user what data was taken, what the data will be used for and to whom the data will be shared with after it has been collected. The policy must also tell the user about the app's data retention policy, including how long the data will be stored and how to delete or opt out of the data collection.

The key to compliance is to obtain the user's consent, before collecting personal data. Thus, the app should provide notice to the user, before the app is downloaded. Given the vague nature of the law's requirements, at least at this point, obtaining consent before a user download's the app is the safest way to comply.

The notice should also provide a clear and easily accessible way to withdraw consent. In a recent California case, the Attorney General for the State of California alleged that a privacy notice was not reasonably accessible when it was contained only on Delta's website, but not in the actual app, "Fly Delta." While this case is still winding through the court system, it should provide some guidance to how accessible a privacy policy should be to avoid legal issues.

Once the app obtains the personal data, the APPS Act requires the developer prevent access to the data. All that the law currently requires is that "reasonable and appropriate measures" are used to prevent un-authorized access to the personal data and de-

identified data. You can certainly speculate that, as drafted, the current law leaves wide open what is or is not appropriate safeguards.

If data has been lost after the APPS Act becomes law, this section will likely be a heavily litigated area. Did the developer design the app with sufficient security measures? Did the app's owner modify the security measures? Given the ever-changing nature data security, what was "reasonable" at one time, is likely going to be unreasonable the following week.

As if it was not confusing enough, the APPS Act still requires mobile app developers to comply with other Federal and State laws. For example, compliance with the APPS Act does not relieve compliance with the Children's Online Privacy Protection Act (COPPA) at the Federal level, or even the California Online Privacy Protection Act (CalOPPA) at the State level. However, when determining whether to follow the APPS Act or State law, the APPS Act will apply, but only when the APPS Act provides a higher level of transparency, user control, or security of personal and de-identified data than the State law.

THE ULTIMATE SAFE HARBOR: NTIA'S CODE OF CONDUCT

The Apps Act does exempt mobile app developers from complying with its provisions, so long as the company complies with the enforceable code of conduct agreed upon through the NTIA's multistakeholder's process. In June 2012, the NTIA announced the goal of the first multistakeholder process was to "develop a code of conduct to provide transparency in how companies providing applications and interactive services for mobile devices handle personal data."

As of April 30, 2013, NTIA published a draft of conduct. Currently, the code of conduct requires short form notices to include information similar to the APPS Act. The code does give examples of third parties with whom data may be shared which require disclosure. The code also provides insight into the design of the notice. In addition to requiring a short form notice, the code requires linkage to long form notices.

The process of drafting the code is set to continue throughout the year in meetings occurring during May and June 2013. Thus, while the code has not been set yet, leaving mobile app developers to wonder how and if they will be exempt, the APPS Act of 2013 has yet to enacted into law – so there is time.

WHO AND HOW WILL THE APPS ACT BE ENFORCED?

The FTC will enforce the APPS Act under sections prohibiting unfair or deceptive acts or practices. A state Attorney General, can enforce the APPS Act through a federal civil action. However, a state could not file a civil action if a federal action is already pending. However, given the recent dismissal of a case brought by California's Attorney General against Delta Airlines, there is another possible agency, which may enforce the APPS Act. According to a California court, the Department of Transportation, not the State of California, regulates how airlines communicate with their customers, even if the customers are in California.

WHAT DOES THE FUTURE HOLD?

At this point, neither the APPS Act of 2013 or NTIA's code of conduct must be complied with until 2014. The APPS Act must proceed through the usual legislative process. There is a chance, of course, that it may not ever become law. The best course of conduct for mobile app developers is to insure they provide input at the committee level during the legislative process. Additionally, monitoring the results of NTIA's May and June 2013 meetings will likely be highly informative. ❖

The key to compliance is to obtain the user's consent, before collecting personal data.

Adam Grant

Adam is a partner with Alpert, Barr & Grant, A Professional Law Corporation. With over 20 years of experience, he supports the firm's litigation practice with expertise in complex business disputes, mobile app law, privacy and embezzlement issues, construction law and real estate matters. He has litigated in both state and federal courts.