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

On the Eighth Day of Privacy, My Mobile Apps Know Everything About Me . . .

Article By:

Privacy & Security Practice Group at Mintz Levin

Of all the "Days of Privacy" looking forward to 2014, we believe that the issues surrounding mobile applications and privacy will see some of the most intense regulatory focus …. read on, and be prepared….

One could argue that the guiding principle behind the exponential growth and pervasive influence of the mobile application industry has been that it is limited only by our imagination's ability to identify tiny new problems to solve, like how to pick the ripest watermelon and how to be a less terrible person while using Google+ video chat. And yet, 2014 could be a year in which regulatory efforts and critical market forces are as notable as the technological innovations, as increased enforcement efforts, greater consumer awareness and certain compliance difficulties unique to mobile applications create a "perfect storm" of potential liability.

In the past few months, state and federal regulatory agencies have continued to publish policy rationales for directing resources toward mobile application privacy. In February, the Federal Trade Commission released a Staff Report focused entirely on mobile technology in which the FTC made it clear that all parties involved in the mobile industry share responsibility for ensuring that appropriate consumer protections are in place. California released a similar report after laying groundwork formore than a year to ensure that California's data privacy regulations, which are among the toughest in the nation, would be applicable to mobile applications. In each case the reports hinted strongly at increased enforcement efforts and in the past few weeks we have been given a clearer view of what such increased enforcement efforts will look like.

The office of New Jersey Acting Attorney General John J. Hoffman announced a settlement agreement with California-based mobile application developer Dogokeo, Inc. in connection with its "Dokobots" application. The Dokobots app was a scavenger hunt game that utilized geolocation data to direct users toward animated cartoon Dokobots and other digital items. The state alleged that Dokogeo's collection of information through its mobile application violated the federal Children's Online Privacy Protection Rule (COPPA) and the Federal Trade Commission's COPPA Rule because the Dokobots application was directed to children and failed to obtain verifiable parental consent prior to the collection of personal information from children. Dokogeo allegedly also failed to link to its privacy policy on its homepage so that parents and other users would be able to find information regarding Dokogeo's data collection practices. Under the terms of the settlement agreement,

Dokogeo is required to (i) clearly and conspicuously disclose, in its mobile applications and on the homepage of its website, information regarding its collection, disclosure and use of information, (ii) verify that all persons using any of its mobile applications that collect personal information are over the age of 13, (iii) remove certain information regarding children from its website and (iv) otherwise comply with the requirements of COPPA and the COPPA Rule as they pertain to online services directed to children. The settlement also includes a suspended settlement payment of $25,000, which Dokogeo will be required to pay if it fails to comply with the terms of the settlement, or otherwise violates COPPA orNew Jersey's Consumer Fraud Act at any point during the 10 year period following the date of the settlement.

Less than a month later, the FTC announced a proposed consent agreement with Goldenshores Technologies, LLC. Goldenshores Technologies marketed the "Brightest Flashlight Free" mobile application, a free mobile application that, according to the proposed consent agreement, has been downloaded tens of millions of times. The FTC alleged that Goldenshores Technologies engaged in unfair and deceptive practices by failing to disclose that certain data, including geolocation data and persistent device identifiers, would be collected by the application and shared with third parties. The FTC also alleged that the collection of data by the application commenced prior to the user's acceptance of the app's end user license agreement. Under the terms of the proposed consent agreement, Goldenshores Technologies is required to, among other things, (i) update its disclosures with respect to the collection, use and disclosure of information, (ii) specifically disclose how geolocation information is used, why it is collected and with whom it is shared, (iii) delete personal information of users collected prior to the date of the consent agreement and (iv) maintain, for a period of 5 years following the date of the consent agreement, certain advertising and promotional materials containing representations about data collection, user complaints and inquiries, and documentation showing compliance with the consent agreement.

The varying allegations in the Dokogeo and Goldenshores Technologies agreements highlight the difficulties mobile applications face in complying with state and federal regulations. On one hand, the extremely personalized nature of data collected by mobile phones mandates heightened protections and disclosure. On the other hand, the complex and multi-layered support structure for most mobile applications (not to mention the smaller screen size) can make it difficult to fully describe the extent to which data is shared with third parties, and create unforeseen security risks. One recent report, for example, found that the majority of mobile applications are vulnerable to hackers because of serious security flaws related to a combination of over-collection of personal data and incorrect implementation of encryption measures, while another report found vulnerabilities in apps that access data using public Wi-Fi networks. In addition, the application of certain sector-specific laws, such as Dokogeo's alleged violation of COPPA, are a particular risk for mobile applications because the use of animated characters and kid-friendly themes (both of which were a factor in the Dokogeo settlement agreement) are commonly used by mobile applications to entice adults.

At the same time, we have seen an increase in media coverage of mobile data privacy issues. The information leaked by Edward Snowden has kept stories related to collection of personal informationsquarely on the front pages and over Black Friday there were numerous stories describing the use ofmobile device tracking by retailers. On the editorial pages concerns persist that consumers do not realize how much private information is being collected by smart phones. As a result, a substantial increase in the number of class action claims against mobile applications in 2014 is not merely possible, but likely.

With that in mind, on this 8th day of privacy, here are 7 steps you can take to help reduce liability in connection with your mobile application or online service in 2014:

1. Reassess your security measures. 2014 will also bring new data breach notification requirements. If your business is newly subject to any such requirements, understanding your risk profile will require a fresh look at how secure your system is.
2. Understand how your customers' information is used and shared. Providing full and accurate disclosure to users requires understanding who you share information with and how those third parties use and share the information. This includes sharing with service providers in ways that may otherwise be considered "routine" in your industry. Also, be sure that you understand how those third parties protect the information you share.
3. Not just "how" and "what", but "why". The requirements under the Goldenshores Technologies consent agreement show that it isn't enough to simply disclose that information may be collected. Effective notice requires that users be informed why information is being collected.
4. Consider deleting what you don't need. The easiest way to reduce your risk profile is to limit what you collect and retain. Consider putting processes in place to collect only what your service requires and to delete information that you no longer need, such as information related to closed accounts.
5. Consider context, not just consent. As we discussed after New York Comic Con was criticized for hijacking attendee Twitter accounts, the expectations of users regarding data collection should be considered as a separate issue from obtaining user consent. In considering whether to bring an enforcement action, it is likely that the FTC considered how many of Goldenshores Technologies' flashlight users would be surprised to learn how much geolocation data the "free" flashlight required.
6. Consider your audience. Whether a service is "targeted to children" may seem like a simple concept generally, but it can be difficult to apply to specific examples, particularly in the realm of games and entertainment. As we describe in our guide to compliance with the amended COPPA Rule, there are a number of factors that should be considered when determining whether a Web site or online service or portion thereof is directed to children.
7. Have a plan for when the worst occurs. Data breaches are considered "one of the unfortunate realities of doing business today". The moment when you discover there has been a data breach is not the time to figure out your plan for what to do when you have a data breach. There's no time like the present to put a game plan in place that can be used in the event of an emergency.

National Law Review, Volume III, Number 353

Source URL:https://natlawreview.com/article/eighth-day-privacy-my-mobile-apps-know-everything-about-me