**Consent for Geo-Positional Data**

TO: Monica Zent

FROM: Alexander Cervantes

DATE: July 30, 2012

RE: Consent for Geo-Positional Data

Question Presented

Does an app licensor have to seek the user’s consent/opt in before pulling geo-positional data from the user’s phone?

Brief Answer

 App licensors do have to seek the user’s consent before they can pull any location data from users’ mobile phones. And the best way to get this consent is by providing an opt in option before fully downloading the app along with the required Privacy Policy that provides clear and complete information regarding how personal data is collected, used, and shared.

**I. Introduction**

With our passage into the technological age our lives have been greatly ameliorated. We can do things faster and better than ever before. With the emergence of the Internet we now have databases of information at the access of our fingertips. However, such great technology does have its tradeoffs, and because it is moving at such a quick rate some issues about its capabilities need to be addressed. Especially dealing with the dwindling amount of privacy.

The Internet is now available to mobile phones and the way certain downloadable applications, “apps”, use the Internet has raised some issues. One of these issues is geo-positional data. The app pools in information about the user’s location and uses the information to either provide assistance or suggestions that correlate with the app’s functions in relation to the user’s geographical position. For instance the “AroundMe” app gathers location data to figure out the gas stations or restaurants nearest you. For some apps it is necessary to gather this information in terms of its function. But “many users aren't aware that popular iPhone apps [like] ‘Paper Toss’ – a game in which you score points for virtually tossing paper in a bin - collects their location data… some app providers and developers sell their users' location data to marketing companies, allowing profiles to be built for targeted advertising and other purposes not necessarily apparent from use of the original app” (TaylorWessing.com). This is what gets consumers heated about apps gathering their geo-positional data.

**II. Analysis**

**Required Privacy Policy**

According to The California Online Privacy Protection Act (Business and Professions Code section 22575) “an operator of a commercial web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial web site or online service shall conspicuously post its privacy policy.” This act provides transparency to the consumer and gives them more control over their privacy and their device’s data.

 There have been various cases involving suits between Apple and it customers dealing with this issue. In these cases Apple failed to provide a “clear” Privacy Policy and collected location data even though the consumer opted out by turning it “off”. In re IPHONE APPLICATION LITIG. Case No. 11–MD–02250–LHK, the Plaintiffs claims against Apple for violations of

California's Unfair Competition Law (UCL) and California's Consumer Legal Remedies Act (CLRA) were their only claims to survive the motion to dismiss. Because Apple did provide a policy, though unclear, they were safe from other serious suits. However, the company did explicitly go against the law in ignoring the consumer “opt outs”.

 In February 2012, Attorney General Kamala D. Harriss recently secured a global agreement to strengthen consumer privacy protection involving huge corporations who create apps. The agreement urged the companies to follow “a statement of principles to foster innovation in privacy protection, promote transparency in privacy practices, and facilitate compliance with privacy laws in the mobile arena,” (Office of the Attorney General). At the first of the list was having a posted privacy policy that explicitly stated the terms. Harriss later went on calling for measures with greater transparency and discussed in detail how to deal with non-compliance. She ended the article suggesting that companies work together to develop a system of best practices.

**Regulations**

The EU and UK have their own laws regarding the regulation of location data but their measures and regulations can serve as a basis for American corporations. “The ‘e-Privacy Directive’ (2202/58/EC) has been implemented locally in the UK by regulation 14 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PEC Reg). This states that location data may only be collected and used if the user cannot be identified by the data; **OR** it is necessary for the provision of a value-added service (e.g. the app or the service provided by means of the app) **AND** the user has given his or her consent.” (TaylorWessing.com).

**Best Practices**

Technology is growing at such a fast rate and the law is struggling to keep up. In order to stay on the safe side and be spared of suits, a developed a system of best practices needs to be followed. According to the Symposium On Usable Privacy and Security, remarks of Commissioner Julie Brill, this framework is “intended to articulate best practices for companies that collect and use consumer data, including social media companies, app developers and of course, many other types of companies as well.”

*(1) we call for companies to build privacy and security protections into new products.*

*(2) we call for simplified choice for businesses and consumers. Consumers should*

*be given clear and simple choices, and should have the ability to make decisions about their information at a relevant time and context.*

*(3) we call for greater transparency. Companies should provide more information about how they collect and use the personal information of consumers.*

Brill goes on to say that developing “Do Not Track” systems in which you could just click or turn on so as to halt the app licensor from collecting data would serve as easy, “universal, one-stop mechanisms to enable consumers to control the tracking” (Julie Brill).

 Brian Socolow and Douglas Masters, of Loeb & Loeb LLP have also devised a list of best practices. First of all it is recommended to follow the industry guidelines when using geo-location data or promotions to reach consumers – either by going through The Mobile Marketing Association, The Wireless Association, or The Direct Marketing Association as sources for guidelines that address privacy and location-based services. They also included a clause suggesting the exclusion of children under 13 or make them comply with special regulations. “The Federal Trade Commission recently proposed revisions to its COPPA (Children’s Online Privacy Protection Act) Rule that would expand the Rule to include mobile devices.  This means some mobile applications would need to comply with COPPA’s requirements, including obtaining prior, verifiable parental consent” (Socolow and Masters). Also it is always good to make sure that the disclaimers can be read on mobile devices. Apps on phones that use location based services should have disclaimers and policies that are conspicuous.

**III. Conclusion**

In conclusion, consent needs to be given before any geo-positional data can be pulled by the app licensor. The best way consent can be obtained by using the “opt-in/out” method. It can also be obtained by having them agree to the written privacy policy that can be viewed either via click-wrap agreements or a hyperlink. The Laws that regulate these programs are still evolving, as are consumer expectations when using or participating in these types of apps. Though it is much easier on both parties to get the user to accept to as little as possible, when it comes to privacy these policies are crucial. When devising an app that uses geo-positional data make sure the guidelines are followed and use the best practices modeled.