Written Questions of Senator Jeff Flake
U.S. Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
The Location Privacy Protection Act of 2014
June 11, 2014

Robert Atkinson

1. During the hearing there was considerable discussion of stalking apps but also legitimate tracking apps. Could you explain what you think the difference is between a stalking app and a tracking app?

    a. In addition, at a technical level, is it possible to distinguish between apps that track individuals imperceptibly for legitimate reasons versus illegitimate reasons?

    "Stalking apps" covertly track and report a user's location to another individual without the user's permission and in violation of the laws on stalking. Legitimate tracking apps, such as those designed to monitor the location of a stolen device, child, or employee, similarly track the location of an individual but do so within the bounds of the law. Similarly, apps such as CarrierIQ monitor mobile devices unobtrusively to improve network performance and diagnose network connectivity issues. At a technical level, there is little to no difference between geolocation apps used to stalk individuals and those used for legitimate purposes. Both types of apps collect, transmit, and store location information about the user and make it available to others. The principle difference between these apps is in how they are marketed and what the data are used for and in some case in the level of transparency provided to the user.

2. Would it be useful in the legislation to distinguish between apps that can be used to stalk individuals and those that use geo-location data for other purposes?

    Yes. While there is a group of apps that track and report the location of individuals to other users, the vast majority of apps using geolocation data do not share this information with other end-users. For example, many websites personalize their services based on the user's location, such as for news, shopping, and maps. Other sites use the geolocation data to improve the performance of the phone and/or the network. Other apps allow users to share their location information with others, but this is done in the foreground, such as sharing location information on social networks. These apps bear no resemblance to the stalking apps of concern to the committee and so should be excluded from legislation intended to crack down on stalking apps.

3. In requiring the 24 hour to 7 day notice, the bill applies this requirement to a "covered entity that initially collects geolocation information from an electronic communications device in a manner that the covered entity has reason to believe is imperceptible to the individual using the electronic communications device…" From a technical perspective, how do you define "imperceptible?"

Imperceptible does not mean that there is no way to perceive that the electronic device is collecting geolocation information, only that it is being done so in a manner that is very subtle or difficult to perceive. Unfortunately, the bill does not define how a developer might distinguish what is "imperceptible to the individual using the electronic communications device." There are small signals that developers might argue count towards notifying the user. For example, devices collecting and transmitting geolocation data generally use more processing power which means they tend to run a bit hot and consume battery power more quickly than devices that are not doing so. Likely this is not the threshold the authors of the bill had in mind.

While legitimate apps generally do not actively try to obfuscate their activity from the user, some legitimate apps may run in the background without directly alerting the user they are collecting geolocation data so as to minimize unnecessarily bothering the user. But these apps will still appear in if the user checks the list of running processes, especially using a popular task killer app. Would this level of disclosure meet the threshold for being considered imperceptible?

Or developers could rely on an alert from an icon on the mobile device to signal to the user that geolocation data is being collected. How large does such an icon have to be on a mobile device (and does it matter the size of the screen)? Or does it matter if the developer knows that the user has low vision or no vision? If user testing reveals that users do not understand the meaning of their devices geolocation icon, does the developer have to take additional action? And is notification still considered perceptible if it is buried after 20 other notification on the device's screen? In addition, to what extent is the app imperceptible if the installer can turn off notifications?

These are just a sampling of the type of real-world problems that developers might encounter trying to comply with this law. This is yet another reason why if Congress pursues this legislation, it should narrowly target this bill to a small class of apps where the location data can be accessed by the person installing the app on the phone while also providing a more robust definition of "imperceptible"