Dr. Robert D. Atkinson

President and Founder

Information Technology and Innovation Foundation (ITIF)

"The Location Privacy Protection Act of 2014"

Submitted to

The U.S. Senate Committee on the Judiciary

Subcommittee on Privacy, Technology and the Law

June 4, 2014

Chairman Franken, Ranking Member Flake, and members of the Committee, I appreciate the opportunity to submit testimony regarding the Location Privacy Protection Act of 2014. I am the President of the Information Technology and Innovation Foundation (ITIF). ITIF is a nonpartisan think tank whose mission is to formulate and promote public policies to advance technological innovation and productivity.

The proposed legislation addresses two very distinct and unrelated issues relating to the use of geo-location data: 1) the collection and use of personal geo-location data by third-parties, and 2) the collection and use of personal geo-location data by individuals, especially in situations that might perpetuate domestic violence, stalking, and harassment. Since these issues are unrelated I will address each separately.

Limiting the Collection and Use of Geo-Location Data by Third Parties Would Unnecessarily Stifle Innovation

The last few years have seen tremendous growth in innovation around location-based services driven by the availability of low-cost mobile devices and ubiquitous wireless connectivity. Location-based services use data about the location of a user's electronic device to deliver personalized applications and services, such as location-based social networking, entertainment, personal fitness, dating, advertising, and search, among many others. These location-based services may use a variety of techniques, including GPS and triangulation from cell towers or Wi-Fi networks, to determine an individual device's location. In addition, other techniques such as using IP addresses or user-submitted information may be used to identify a less-precise estimate of a device's location. The proposed legislation addresses the use of geo-location data that is sufficient to identify the street and city where the device is located.

First, given the rapidly developing nature of the market for location-based services it would be premature to pursue legislative changes to create a new set of rules to govern the technology. While there has been substantial change in the market for location-based services in the past few years, another wave of location-based services are likely to emerge in the coming years as a result of multiple technology trends, including the growth in adoption of in-car navigation and "infotainment" systems; connected devices making up the "Internet of Things"; and facial recognition systems. Dynamic technologies that are quickly evolving in response to changes in technological capabilities, consumer demands, and cultural norms do not lend themselves to the slower-moving regulatory process of Congress and federal agencies. A better approach is to rely on industry-led self-regulatory efforts which can more rapidly address potential consumer concerns while also being responsive to changes in technology and the private sector.[1] Government oversight and enforcement by agencies such as the Federal Trade Commission (FTC) supplements these efforts to ensure their effectiveness and accountability.

Self-regulation is already used in areas such as online advertising to govern how geo-location data may be used and shared with third parties. For example, the Digital Advertising Alliance's Self-Regulatory Principles has strong transparency requirements stating that mobile apps must give "clear, meaningful, and prominent" notice if transferring geo-location data to third-parties.[2] Other industry-led efforts have also been effective at addressing many of the most common concerns about the most common uses of geo-location data. For example, the two major mobile device operation systems—iOS and Android—allow users to see whether an app uses geo-

location data both before downloading an app and after installing it. In addition, users can disable location services completely for their devices and for each individual app on their device. These types of settings allow users who are concerned about the privacy of their location data to make informed choices about whether it is disclosed.

Codifying current practices in legislation limits the ability to introduce future innovation, including new business models and new technologies. For example, while it is fairly straightforward for mobile apps to provide notifications to users on mobile devices via their touchscreens, not all connected devices in the future will have these types of interfaces. The coming years will likely see a rapid development in connected devices that will make up the Internet of Things, including connected vehicles and wearable computing, and many of these will use geo-location data. It is not obvious how developers of a product like "smart" shoes that collect geo-location information would comply with the notification and consent requirements in the proposed legislation. (Such "devices" could be covered under the legislation since they are "commonly carried by or on the person of an individual".) While these types of devices are less common today, this may not always be the case, and legislation should not preempt these types of products at such an early stage in their development.

Moreover, while notification and consent to use geo-location data is appropriate for mobile apps today, it may not be so for other types of platforms in the future. For example, the use of geo-location information may be so integral to the purpose and functioning of a particular device that mandatory disclosures and consent requirements would be superfluous. The success of products and services often depends, in part, on how easy they are to use. Consumers expect products and services to just work immediately "out of the box." As norms change, many consumers will likely come to expect apps to deliver personalized content based on a variety of information, including their location. Unnecessary alerts, consent requirements, and disclosures make it more difficult to enroll new customers and create a "speed bump" for innovation.

Second, there is little evidence of any actual harms arising from the commercial use of geo-location data. Much of the concern expressed to date by privacy advocates stems from speculative harms, not actual ones. In fact, companies collecting and using the data have strong incentives to not harm consumers, either directly or indirectly, since doing so would badly damage both their reputations and commercial prospects. This is not to say that some companies have not made some mistakes as they seek to innovate, but there is no evidence that these mistakes are either purposeful or a result of negligence. Rather, they reflect that fact that innovation, especially in new spaces like location-based services, is complex and often difficult.

Third, the proposed legislation could discourage many innovators from bringing location-based products and services to the market. The legislation would create a private right of action and allow fines of up to $2 million for violations in how a company discloses or obtains consent about the use of geo-location information, in addition to potentially requiring the defendant to pay the plaintiff's attorney's fees. These stiff penalties, coupled with the motivation for trial lawyers to find and bring cases, will make many risk-averse companies, particularly small companies and startups, avoid using geo-location data in their mobile apps and other devices for fear that inadvertent mistakes could end up with them facing significant liabilities for fines and legal fees, which in many cases would lead to personal bankruptcy.

The consent requirements would also impair the use of geo-location data in some situations. For example, Carrier IQ is a diagnostics and analytics software tool that many carriers install on mobile devices to better understand their customers, the devices used on their networks, and the performance of their networks. Carrier IQ collects data such as when and where calls fail; where customers have problems accessing the network; and the reliability and battery performance of the make and model of devices. This information is then used to improve service quality and answer consumer questions. For example, a service provider's technical support staff can use this data to help better understand and resolve customers' issues, such as a mobile device losing connectivity in a certain location or a tablet PC's battery draining too quickly. If consumers have to opt in to this type of service there will be a strong incentive to "free ride" by not contributing their own data but still benefiting from the overall health of the wireless network based on the information collected from others. Of course, if a significant number of users do not use this type of service all users will suffer the consequences. The same is true with regard to traffic flow data where de-identified data is used to enable real-time traffic maps on roadways; if some individuals opt out, the overall quality of the data for all travelers will decline.

Another type of use that might suffer under this legislation is the use of geo-location in online advertising. Online advertising pays for a significant amount of free content and services that consumers enjoy, including mobile apps. In 2013, online advertisers spent approximately $43 billion, including $7 billion on mobile advertising.[3] However, advertisements need to be effective to justify these significant outlays. This means that advertisers need to be able to use data to deliver relevant advertising and use data to analyze the effectiveness of advertising. Apps that require users to grant them a greater number of permissions are less likely to be downloaded. Requiring apps to get give notices to users about use of geo-location data in advertising would force many developers to make the tradeoff between incorporating useful location data, either to be used directly by the application or for third-party advertising, and potentially scaring off customers. Moreover, many apps are using geo-location data to deliver more relevant advertising to consumers. For example, apps like Yelp and FourSquare allow restaurants and retailers to offer promotions to customers who "check in" to a specific location, and the car service Uber runs promotions to its users based on their geo-location, such as a special discount for attendees at certain events. Geo-location data may also be used to be more sensitive to when customers are shown advertising, such as avoiding showing ads when someone is visiting a cemetery. The effect of limiting the relevance of ads, besides consumer inconvenience, would be to reduce revenues going to the mobile ecosystem, with the result being either fewer or lower quality apps or fewer free apps.

In addition, some of the components of the bill are particularly problematic. The requirement that companies disclose the name of every third party they share geo-location data with, as opposed to general categories of reasons for data sharing, would mean that companies would risk sharing proprietary information about their business models to their competitors.

Limiting the Collection and Use of Geo-Location Data by Individuals Would Be Insufficient to Fully Address Concerns about Domestic Violence, Stalking, and Harassment

Domestic violence, stalking, and harassment are serious issues, and ITIF applauds the Committee's efforts to address this ongoing concern. Unfortunately, the provisions in the proposed legislation, while helping with the problem, will likely not be sufficient to fully address

it, may interfere with legitimate tracking applications, and could require changes in mobile operating systems.

First, the legislation includes a number of "anti-stalking provisions" that might be useful for apps that collect and report back to users their geo-location information, but would be applied too broadly to all apps using geo-location data. For example, the legislation requires that users be alerted after more than 24 hours but before 7 days that their geo-location information is being collected. As written, this provision would apply to many different background apps that use location-based services, not just "stalking apps." For example, Passbook is an app on iOS that organizes information, such as boarding passes, movie tickets, and gift cards, and then presents that information automatically to the user when they arrive at the associated location (such as an airport).[4] This type of app runs in the background and is arguably "imperceptible to the user", thereby meeting the definition of the proposed legislation. Delayed notification that geo-location information is being collected for this type of app does not make sense and will only serve to confuse users. Indeed, most apps that collect geo-location information, such as weather or traffic apps, do not allow the individual user to gain access to the information. This is in contrast to apps like Amber Alert GPS Teen, that lets parents download a tracking app on their children's mobile device and track the device's location. As such, we recommend that if the Committee moves forward with this provision, it only apply the 24 hour-7 day second notification rule to apps where individuals can gain direct access to the location data.

Second, even requiring apps to display a delayed notice, however, may not limit stalkers. This is because the delayed notification requirement presents a technical challenge since both the Android and iOS operating systems allow users to turn off notifications.[5] In other words, a stalker who places a tracking app on another person's mobile device could simply shut off notification from that app. For the after-installation notice provision to be fully effective, this legislation would need to require changes to these operating systems to allow third-party app developers to override user preferences about notification settings. Moreover allowing developers to override user preferences could result in a degraded mobile experience as developers may provide notices to users who do not want them and decide to start showing users other notifications, not just geo-location privacy notices.

Third, because the Internet is global, even if Congress successfully bans tracking apps in the United States, users will still likely be able to access them on foreign web sites. This is particularly problematic for mobile devices that allow apps to be installed from any location (i.e. not just from an "authorized" app store). For example, a foreign app store may sell apps that are designed to help parents keep track of their teenage children but that does not include the 24 hour-7 day second notice requirement In some cases it may be appropriate for the U.S. government to require that access to certain websites be blocked (such as a website only selling apps that are illegal in the United States), but in other cases, such as when a site is selling many different apps and products and the vast majority are lawful, it would be inappropriate to block access on such a wide scale.

Fourth, even if the delayed notification provision does help with regard to mobile apps, there are other technologies that stalkers can use, such as portable GPS devices, many of which are used for legitimate purposes. For example, the Amber Alert GPS Smart Locator is a standalone device that parents can place in a child's backpack in order to keep track of the child's location.

These same devices could also be placed in a person's car by a stalker. It is not clear how these devices could meet the notification and consent requirements in the legislation.

Fifth, as this above example illustrates, at a technical level there is little difference between a stalking app and a legitimate app that tracks an individual device's location and reports this information to that individual or another user. Legitimate examples of tracking include apps designed to find lost or stolen electronics, apps designed to create a "geo-fence" for teenage drivers, and apps designed to track the location and safety of loved ones who are unable to live independently, such as parents with early stages of dementia or adults with cognitive disabilities. In particular, some parents have troubled children who they may feel they need to track to provide proper supervision. If the children know that they are being tracked, they may simply leave their phone at home, school or with a friend. This is not to say that this provision should not be enacted, only that it would also prevent this kind of beneficial tracking without the person's knowledge.

Unfortunately, it is virtually impossible to restrict one type of tracking app but not another. Congress could and should ban the marketing and sale in the United States of apps advertised and marketed as stalking apps, but that would not prevent would-be stalkers from using a legitimate tracking app for "off-label" purposes. Moreover, tracking itself is not a problem; rather, the problem is its use by stalkers. After all, a number of apps use geo-location data to protect the personal safety of individuals, such as by sharing personal geo-location data with trusted friends and family. One mobile app, which was a winner in the 2011 HHS / White House "Apps Against Abuse" Challenge, allows users to quickly and surreptitiously request that friends pick them up by sharing their precise geo-location.[6] Another app, the "Safety Siren", developed by YWCA Canada, allows users to quickly send a text or email to friends with their location information if they are in an unsafe situation.[7] Some states have begun to use geo-location data to turn the tables on stalkers and ensure that victims and police are alerted of possible threats. As of 2012, at least twelve states already have laws that require certain offenders to wear a tracking device so that police and victims can be alerted if the offender violates a protective order.[8] ITIF encourages Congress to consider efforts to expand the number of states using GPS tracking devices to protect those individuals threatened with domestic violence or other illegal harassment, including through grants from the Department of Justice.

In addition, Congress should be aware that advances in mobile security may help address some of the concerns about surreptitious stalking apps. These types of apps are a form of malware—malicious programs installed without the users knowledge. There are other types of malware including keyloggers (that steal private information, such as credit card numbers and passwords) as well as backdoors that allow remote access to a device. Many users are concerned about these types of security threats and developers are responding by developing improved security tools for mobile devices. In the coming years, we will likely see more anti-virus and anti-malware tools for mobile devices just like there are for PCs. These tools will likely address a variety of malware threats, including stalking apps. In addition, mobile operating system developers will continue to add new security features, such as biometric authentication requirements that would help prohibit apps from being installed on a user's device without their biometric "permission."

In the short term, individuals concerned that third-parties may have access to their mobile devices and are using this access to track them can take a number of steps to protect themselves

including changing the passwords for their mobile devices and associated accounts; installing anti-malware and anti-virus apps; and even disabling all location-based services in the mobile device's operating system. The Department of Justice should work with victims' assistance organizations to ensure that these kinds of self-help practices are widely understood.

Conclusion

In summary, geo-location data offers many opportunities for innovation in the coming years and efforts to regulate its use for commercial purposes will do little to protect consumers and are likely to limit continued innovation. In addition, the Committee should also be aware that even the stalking provisions will not be a "magic bullet" for stopping electronic stalking, in part because stalkers can turn off notification and also use other kinds of devices not covered here. Given the concerns expressed above about the impact that this legislation would have on voluntary and legitimate uses of geo-location data by third parties for innovative applications and services, I recommend the committee not move forward with Section 3 of the legislation and instead focus its efforts on criminal penalties for stalking as outlined in Section 4 and the other measures in Sections 5 through 10.

Endnotes

---

1. Daniel Castro, "Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising," (Information Technology and Innovation Foundation, December 2011), http://www.itif.org/files/2011-self-regulation-online-behavioral-advertising.pdf.

2. "Application of Self-Regulatory Principles to the Mobile Environment," Digital Advertising Alliance, July 2013, http://www.aboutads.info/DAA_Mobile_Guidance.pdf.

3. "2013 Internet Ad Revenues Soar To $42.8 Billion, Hitting Landmark High & Surpassing Broadcast Television For The First Time—Marks a 17% Rise Over Record-Setting Revenues in 2012", Internet Advertising Bureau, April 10, 2014, http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-041014.

4. For more on Passbook, see http://support.apple.com/kb/HT5483.

5. For Android see, "How To Shut Off Android Notifications," Digital Trends, September 3, 2012, http://www.digitaltrends.com/mobile/how-to-deal-with-android-notification-spam/. For iOS see, "" "iOS: Understanding notifications," Apple, January 17, 2014, http://support.apple.com/kb/ht3576.

6. See Circle of 6 at http://www.circleof6app.com/.

7. See YWCA Safety Siren at http://ywcacanada.ca/en/pages/mall/apps.

8. Daniel Castro, "Location Privacy Legislation is Move in Wrong Direction: Part 2 – Stalking and Domestic Violence", Information Technology and Innovation Foundation, January 14, 2013, http://www.innovationfiles.org/location-privacy-legislation-is-move-in-wrong-direction-part-2-stalking-and-domestic-violence/.