Oral Testimony of Ashkan Soltani (as delivered)

Independent Privacy Researcher and Consultant

United States Senate, Judiciary Subcommittee on Privacy, Technology and the Law

Hearing on

Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy

May 10, 2011

Chairman Franken, Ranking Member Coburn, and distinguished members of the Subcommittee. Thank you for the opportunity to testify about mobile privacy and the location ecosystem.

My name is Ashkan Soltani. I am a technology researcher and consultant specializing in privacy and security on the Internet. As background, I served for a year as a technologist in the Division of Privacy and Identity Protection at the Federal Trade Commission. I was also the primary technical consultant on the Wall Street Journal's *What They Know* series.

I should note: the opinions here are my own and don't reflect the views of my previous employers.

Mobile devices today—are powerful computing machines. But unlike desktop computers, mobile devices introduce unique privacy challenges. Consumers carry their phones and tablets with them almost everywhere they go—from their homes—to their offices—and from daycare to the grocery store.

A devices location can be determined using a number of different technologies, including GPS—information about nearby cell towers and WiFi access points, and other network-based techniques. While the accuracy can vary depending on the technology being used, the resulting insights derived from this data can be sensitive—and personal—in nearly all cases.

If you imagine a historical trail of your whereabouts over the course of many days, it would be reasonably easy to deduce where you work—where you live—and where you play. This information can reveal much—about who you are as a person and how you spend your time.

I believe this is why many consumers have been surprised by recent stories of how their mobile device may be collecting their location information and other sensitive data.

With the exception of GPS, the process by which a device's location is determined can actually expose that location to multiple parties. These parties include: the wireless carrier (for example AT&T and Verizon), the location service provider (such as Apple, Google, and Skyhook), and even the content provider used to deliver information about that location, such as a mapping website or service.

Researchers—including myself—recently confirmed that smartphones, such as Apple iPhones and Google Android devices—send location information quietly in the background to Apple and Google servers, respectively, even when the device isn't actively being used.

That is—background collection happens automatically—unless the user is made aware of the practice and elects to turn it off. This is the default behavior when you purchase these devices.

Furthermore, most smartphones keep a copy of historical location information directly on the device. Until recently, Apple's iPhone would retain a location history log for as long as one year—stored insecurely on the phone—and on any computers the phone was 'backed up to.' Anyone with access to this file would be able to obtain a historical record of your approximate whereabouts and *there was no way to disable it.*

Many mobile smartphones platforms—like Apple iOS and Google Android—also allow third-parties to develop applications for their devices—productivity software like e-mail, social media tools like Facebook, and—of course—games.

As reported in the Wall Street Journal last year, many popular phone "apps" transmit location information or its unique identifiers to outside parties. For instance, if a user opens Yelp—a popular restaurant discovery app—not only does Yelp learn information about the user, but so could Yelp's downstream advertising and analytics partners.

This may be surprising to many consumers—since they may not have an explicit relationship with these downstream partners. <*pause*> This information isn't limited to just location. Upon

installation, many of these apps would have access a users phone number, address book, and even text messages.

Disclosures about the collection and use of consumer information are often ineffective or completely absent. Many disclosures are often vague or too confusing for the average consumer to understand—and they rarely mention specifics about data retention and information sharing practices that a privacy conscious consumer would care about. Notably—nearly half of the popular apps analyzed by the Wall Street Journal lacked discernible privacy policies.

To conclude—in order to make meaningful choices about their privacy, consumers need increased transparency into who's collecting their information about them and why. Clear definitions should be required for sensitive categories of information—such as location and other identifiable information. Software developers need to provide consumers with meaningful choice and effective opt-outs that allow consumers to control who they share information with and for what purpose.

Only in an environment that fosters trust and control will we be able to take advantage of all the benefits mobile technologies have to offer.

I thank the subcommittee for inviting me here to testify today, and I look forward to answering any questions you may have.