Testimony of Alan Davidson, Director of Public Policy, Google Inc.

Before the Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
"Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy"

May 10, 2011

Chairman Leahy, Chairman Franken, Ranking Member Coburn, and members of the Committee:

I am pleased to appear before you this morning to discuss mobile services, online privacy, and the ways that Google protects our users' personal information. My name is Alan Davidson, and I am a Google's Director of Public Policy for the Americas. In that capacity, I oversee our public policy operations in the United States, and work closely with our legal, product, and engineering teams to develop and communicate our approach to privacy and security, as well as other issues important to Google and our users.

Google is most well known for our search engine, which is available to Internet users throughout the world. We also make Android, an open operating system for mobile devices that in a few short years has grown from powering one device (introduced in the fall of 2008) to over 170 devices today, created by 27 manufacturers. We also offer dozens of other popular services, from YouTube to Gmail to Google Earth. Our products are generally offered for free for personal use, and one supported by revenue from advertising and sales to businesses.

Protecting privacy and security is essential for Internet commerce. Without the trust of our users, we simply would not be able to offer these services or platforms because on the Internet, competing services are only one click away. If we fail to offer clear, usable privacy controls, transparency in our privacy practices, and strong security, our users will simply switch to another provider. This is as true for our services that are available on mobile devices as it is for those that are available on desktop computers. For this reason, location sharing on Android devices is strictly opt-in for our users, with clear notice and control.

In my testimony today, I'll focus on three main points:

- Location-based services provide tremendous value to consumers;
- Google is committed to the highest standards of privacy protection in location-based services; and
- Congress has an important role in helping companies build trust and create appropriate government access standards.

I. <u>Location based services provide tremendous value to consumers</u>

Mobile services are creating enormous economic benefits for our society. A recent market report predicts that the mobile applications market will be worth $25 billion by 2015. At Google, we have seen an explosion in demand for location-based services.

People can use our services to find driving directions from their current location, identify a traffic jam and find an alternate route, and find the next movie time at a nearby theater. Location can even make search results more relevant: If a user searches for "coffee" from a mobile phone, she is more likely to be looking for a nearby café than for the website of a national coffee chain or the Wikipedia entry describing coffee's history. In the last year, a full 40% of Google Maps usage was from mobile devices. There are now 150 million active monthly Google Maps for Mobile users on Android, iPhone, BlackBerry, and other mobile platforms in more than 100 countries.

Many third party applications also use location services to provide helpful products. For example, the U.S. Postal Service offers an application to help users find nearby post offices and collection boxes, based on their location. And if you want a Five Guys burger, their application will find a location for you, and even lets you order and pay in advance. Twitter allows users to "geotag" their tweets from their application, which can give followers important context and perspective. On smartphones like iPhone, Palm, and Android devices, services such as Yelp and Urbanspoon use location to provide relevant local search results, while applications like Foursquare let users find nearby friends.

Mobile location data can even save lives. In the past, a parent's best hope of finding a missing child might have been a picture on a milk carton, but mobile location services may be changing that. Google works with the National Center for Missing and Exploited Children (NCMEC) in an ongoing partnership to develop technology solutions that help them achieve their mission. Today, modern tools and information can make NCMEC's AMBER alerts more effective and efficient by sending the alert to all users within one mile of an incident within seconds of the report through location-based targeting. Over time, the radius could be expanded, with speed and acceleration of distribution based directly on information received.

Existing emergency notifications like AMBER alerts can be improved using location data. In crisis situations, people are increasingly turning to the Internet on mobile or desktop devices to find information. Within a few hours of the Japan earthquake, for example, we saw a massive spike in search queries originating from Hawaii related to "tsunami." We placed a location-based alert on the Google homepage for tsunami alerts in the Pacific and ran similar promotions across News, Maps, and other services. In cases like the Japanese tsunami or the recent tornadoes in the U.S., a targeted mobile alert from a provider like Google or from a public enhanced 911 service may help increase citizens' chances of getting out of harm's way.

None of these services or public safety tools would be possible without the location information that our users share with us and other providers, and without the mobile platforms for businesses and governments to effectively reach the appropriate audience.

II. Google is committed to the highest standards of privacy protection in location-based services

Google would not be able to offer these services or platforms or help create the economic and social value generated from location data if we lost the trust of our users. Thus, at Google, privacy is something we think about every day across every level of our company. It is both good for our users and critical for our business.

Privacy at Google begins with five core principles, which are located and available to the public at www.google.com/corporate/privacy_principles.html:

- Use information to provide our users with valuable products and services.
- Develop products that reflect strong privacy standards and practices.
- Make the collection and use of personal information transparent.
- Give users meaningful choices to protect their privacy.
- Be a responsible steward of the information we hold.

As with every aspect of our products, we follow the axiom of "focus on the user and all else will follow." We are committed to using information only where we can provide value to our users. That's what we mean by our first principle.

For example, **we never sell our users' personally identifiable information**. This is simply not our business model.

To further guide us, under the second principle, we aim to build privacy and security into our products and practices from the ground up. From the design phase through launch, we consider a product's impact on our users' privacy. And we don't stop at launch; we continue to innovate and iterate as we learn more from users.

Our last three principles give substance to what we mean by privacy: We commit to *transparency*, *user control,* and *security*.

Internal process and controls

We also reflect these principles in our development process and employee training. As consumers become more reliant on services provided by third parties, consumer privacy relies increasingly on those parties' internal practices, process, and controls. As we recently explained, we have begun to implement even stronger privacy controls with a focus on people, training, and compliance.

We have developed a review process where all engineering projects leads are required to submit and maintain a Privacy Design Document detailing how their projects handle user data. These documents are reviewed by cross-functional working groups that can request code reviews and make recommendations to the product teams. Completion of Privacy Design Documents will also be reviewed by managers and an independent internal audit team. We have also enhanced our core training for engineers and others to create a greater focus on responsible collection, use, and handling of data.

All this process is aimed at ensuring that products match our philosophy and avoid mistakes that fracture user trust — like the launch of Google Buzz — which fall short of our standards for transparency and user control. To help make sure we live up to this promise, we entered into a consent decree with the Federal Trade Commission this year, under which we'll receive an independent review of the privacy procedures we have outlined above once every two years. In addition, we'll ask users to give us affirmative consent before we change how we share their personal information.

How our products reflect our principles — Opt-in controls on Android

Moving to our specific products, I'll focus first on an important area in which we are putting our principles to work, and where we are innovating on the broader privacy issues faced in the online world: Simple, opt-in controls for collection and use of location information on Android.

While location-based services are already showing great value to users, Google recognizes the particular privacy concerns that come with the collection and storage of location information. That's why we don't collect any location information — any at all — through our location services on Android devices unless the user specifically chooses to share this information with Google. We also give users clear notice and control; the set-up process asks users if they would like to "allow Google's location service to collect anonymous location data."

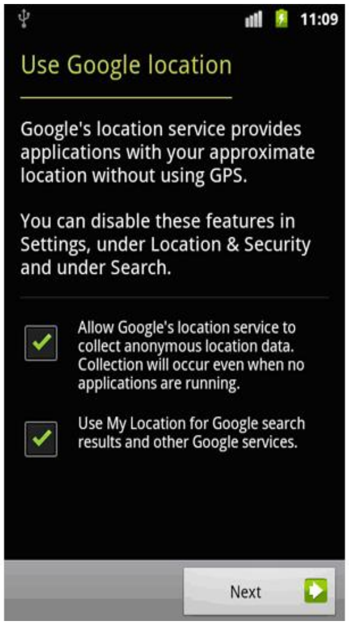
And even after opting in, we give users a way to easily turn off location sharing with Google at any time they wish. The location services in our Android operating system embody the transparency and control principles that we use to guide our privacy process.

Google is also very careful about how we use and store the data that is generated by location-based services. The location information sent to Google servers when users opt in to location services on Android is anonymized and stored in the aggregate and is not tied or traceable to a specific user. The collected information is stored with a hashed version of an anonymous token, which is deleted after approximately one week. A small amount of location information regarding nearby Wi-Fi access points and cell towers is kept on the Android device to help the user continue to enjoy the service when no server connection is available and to improve speed and battery life. This information on the device is likewise not tied or traceable to a specific user.

Global Positioning System (GPS) enabled devices can provide a highly accurate location using information from GPS satellites. But GPS can be slow and drain battery life and can take 10 seconds (and sometimes much longer) to "fix" a location. Furthermore, many devices are not GPS enabled or are used in situations where obtaining a GPS signal might not even be possible (*e.g.*, indoors, where there is no line of sight between the device and the satellites).

In order to serve devices that may not have GPS capabilities, or simply to avoid the delay and battery drain from GPS services, various companies have worked out alternatives to GPS. These are generally based around the idea of detecting nearby, publicly available signals from Wi-Fi access points and cell towers and using this data to quickly approximate a rough position, usually with less accuracy than GPS. By treating Wi-Fi access points or cell towers as beacons, devices are able to fix their general location quickly in a power-efficient way, even while they may be working on a more precise GPS-based location. This can be done by using information that is publicly broadcast (for example, that list of Wi-Fi access points you see when you use the "join network" option on your computer). A database of known network locations is required to determine a user's estimated location from either Wi-Fi access point or cell tower information. Companies like Skyhook Wireless and Navizon compile such databases and license the data to many industry leaders.

Google has also created such location service called the Google Location Server — an Internet database on Google servers that uses Wi-Fi access points and cell towers to determine an estimated location and that uses GPS information to estimate road traffic. Device manufacturers can install the Google Network Location Provider application for Android (pursuant to a license with Google) on their devices. This application can determine a user's estimated location using the Google Location Server, to make location information available to users whether they are indoors and outdoors, more quickly, and using less battery power than GPS services. This Network Location Provider is turned off by default, and can be turned on by the user during the phone's initial setup or in the device settings.



Use Google location

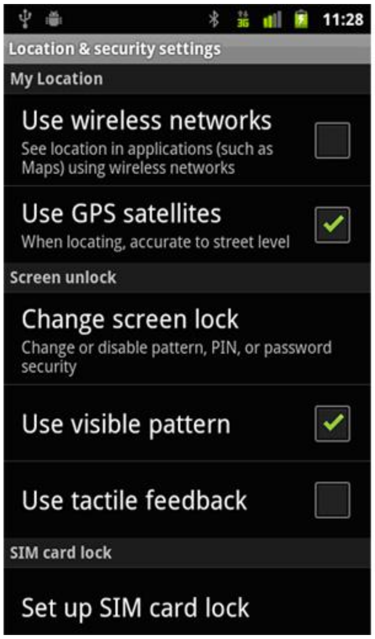
Google's location service provides applications with your approximate location without using GPS.

You can disable these features in Settings, under Location & Security and under Search.

☑ Allow Google's location service to collect anonymous location data. Collection will occur even when no applications are running.

☑ Use My Location for Google search results and other Google services.

The Network Location Provider is off by default. The user can opt-in and turn on location services during the initial setup flow.



11:28

Location & security settings

My Location

Use wireless networks ☐
See location in applications (such as Maps) using wireless networks

Use GPS satellites ☑
When locating, accurate to street level

Screen unlock

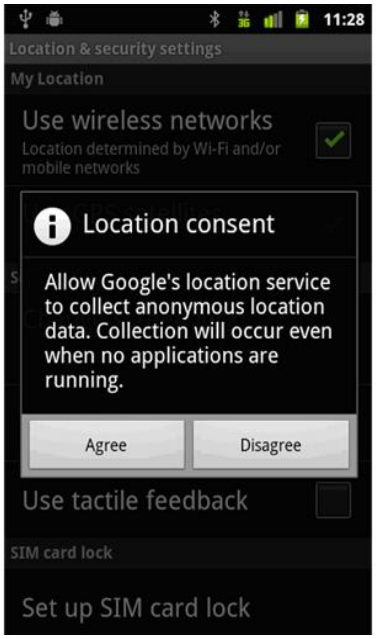
Change screen lock
Change or disable pattern, PIN, or password security

Use visible pattern ☑

Use tactile feedback ☐

SIM card lock

Set up SIM card lock



11:28

Location & security settings

My Location

Use wireless networks ☑
Location determined by Wi-Fi and/or mobile networks

Location consent

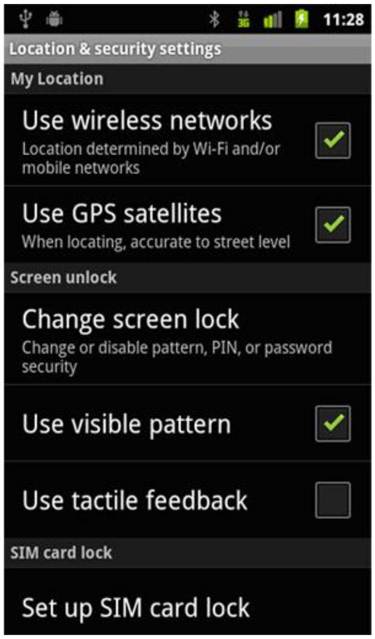
Allow Google's location service to collect anonymous location data. Collection will occur even when no applications are running.

Agree | Disagree

Use tactile feedback ☐

SIM card lock

Set up SIM card lock



11:28

Location & security settings

My Location

Use wireless networks ☑
Location determined by Wi-Fi and/or mobile networks

Use GPS satellites ☑
When locating, accurate to street level

Screen unlock

Change screen lock
Change or disable pattern, PIN, or password security

Use visible pattern ☑

Use tactile feedback ☐

SIM card lock

Set up SIM card lock

The user can opt-in to turn on the Network Location Provider on their Android phone from within the device settings.

The Android operating system is built on the principle of openness, with the goal of encouraging developer innovation and a vibrant ecosystem for users. With this principle in mind, Google does not decide which applications can access location or other user information from the device. Instead, the Android operating system uses a permissions model in which the user is automatically informed of certain types of information an application will be able to access during the application installation process. This permissions model is designed to empower users to make their own decision on whether or not to trust an application with the information requested. The user may choose to trust the application by completing the installation or the user may choose to cancel the installation. An application can only access the device's GPS location or the device's network location if it displays a permission to the user at time of installation.

When Google creates an Android application, like the Google Maps for mobile application, Google is responsible for how the application collects and handles data and for the privacy disclosures made to users. Most Google-developed Android applications are subject to the Google Mobile Terms of Service and the Google Mobile Privacy Policy, unless Google has created a custom terms of service and privacy policy for the application. Google privacy policies are also clearly displayed to the user when the user first signs into the Android device.

When an Android application is not developed by Google, the application developer bears the responsibility for the design of the application, which includes responsibility for how the application collects and handles user data and the privacy disclosures made to users. If the user chooses to trust an application with location information by proceeding with the installation after viewing the location-related permissions, then that application could potentially store this location information on the device or transmit the information off the device if the application also has the Internet access permission. Google does not control the behavior of third party applications or how they handle location information and other user information that the third party application obtains from the device, even though Google strongly encourages application developers to use best practices as described in this Google blog post.

How our products reflect our principles — Encryption and two-step verification

Along with transparency and user control, strong security for users of Google's services to protect against hackers and data breach is vital. Nothing can erode trust faster than personal information falling into the hands of hackers. Google faces complex security challenges while providing services to millions of people every day, and we have world-class engineers working at Google to help secure information.

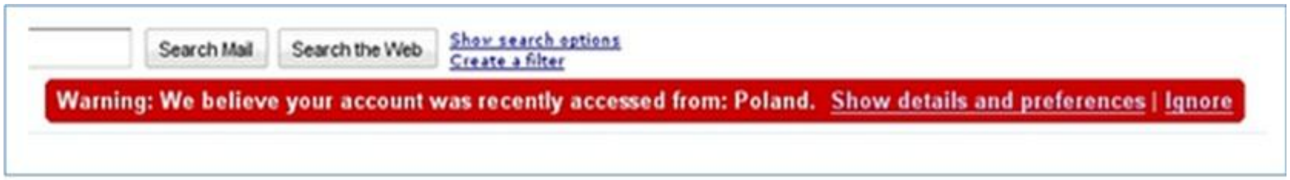
For example, Google is the first (and only) major webmail provider to offer session-wide secure socket layer (SSL) encryption *by default*. Usually recognized by a web address starting with "https" or by a "lock" icon, SSL encryption is regularly used for online banking or transactions. As our Gmail lead engineer wrote:

> In 2008, we rolled out the option to always use https — encrypting your mail as it travels between your web browser and our servers. Using https helps protect data from being snooped by third parties . . . . We initially left the choice of using it up to you because there's a downside: https can make your mail slower since encrypted data doesn't travel across the web as quickly as unencrypted data. Over the last few months, we've been researching the security/latency tradeoff and decided that turning https on for everyone was the right thing to do.

We hope other companies will soon join our lead.

We also hope to see our competitors adopt another security tool we offer our users: encryption for search queries. Users can simply type "https://encrypted.google.com" into their browsers to navigate to the version of Google Search that encrypts search queries and results. As we said in our blog post about encrypted search, "an encrypted connection is created between your browser and Google. This secured channel helps protect your search terms and your search results pages from being intercepted by a third party on your network."

And in March of last year Google introduced a system to notify users about suspicious activities associated with their accounts. By automatically matching a user's IP address to broad geographical locations, Google can help detect anomalous behavior, such as a log-in appearing to come from one continent only a few hours after the same account holder logged in from a different continent. Thus, someone whose Gmail account may have been compromised will be notified and given the opportunity to change her password, protecting her own account and her Gmail contacts.



Warning: We believe your account was recently accessed from: Poland.

Finally, we recently released 2-step verification for consumer Gmail accounts, which allows users who are concerned about the security of their account to use a password plus a unique code generated by a mobile phone to sign in. It's an extra step, but it's one that significantly improves the security of a Google Account. Now, if someone steals or guesses a Gmail user's password, the potential hijacker still cannot sign in to the user's account because the hijacker does not have the user's phone. We are already hearing stories from our users about how this extra layer of security has protected them from phishing attacks or unauthorized access.

III. Congress should act to build trust and create appropriate government access standards

Congress has a vital role to play in encouraging responsible privacy and security practices, both by bringing attention to these issues and through appropriate legislation.

As a start, Google supports the development of comprehensive, baseline privacy framework that can ensure broad-based user trust and that will support continued innovation and serve the privacy interests of consumers. Some key considerations in this area include:

- **Even-handed application.** A pro-innovation privacy framework must apply even-handedly to all personal data regardless of source or means of collection. Thus, offline and online data collection and processing should, where reasonable, involve similar data protection obligations.

- **Recognition of benefits and costs.** As with any regulatory policy, it is appropriate to examine the benefits and costs of legislating in this area, including explicit attention to actual harm to users and compliance costs.

- **Consistency across jurisdictions**. Generally, Internet users neither expect nor want different baseline privacy rules based on the local jurisdiction in which they or the provider reside. Moreover, in many instances, strict compliance with differing state or national privacy protocols would actually diminish consumer privacy, since it would require Internet companies to know where consumers are located at any given time.

We also suggest two concrete areas where Congress can act immediately to strengthen Americans' privacy protections and provide consistency for providers:

We pride ourselves at Google for industry-leading security features, including the use of encryption for our search and Gmail services. But we need help from the government to help ensure that the bad acts of criminal hackers or inadequate security on the part of other companies does not undermine consumer trust for all services. Moreover, the patchwork of state law in this area leads to confusion and unnecessary cost. Congress should therefore promote uniform, reasonable security principles, including data breach notification procedures.

Finally, the Electronic Communications Privacy Act, the U.S. law governing government access to stored communications, is outdated and out of step with what is reasonably expected by those who use cloud computing services. ECPA worked well for many years, and much of it remains vibrant and relevant. In significant places, however, a large gap has grown between the technological assumptions made in ECPA and the reality of how the Internet works today, leaving us in some circumstances with complex and baffling rules that are both difficult to explain to users and difficult to apply.

As part of the Digital Due Process coalition, we are working to address this issue. The Digital Due Process coalition includes members ranging from AT&T to Google to Americans for Tax Reform to the ACLU. It has put forward common sense principles that are designed to update ECPA, while ensuring that government has the legal tools needed to enforce the laws. Particularly relevant to today's hearing, the coalition seeks to:

- **Create a consistent process for data stored online.** Treat private communications and documents stored online the same as if they were stored at home and require a uniform process before compelling a service provider to access and disclose the information.

- **Create a consistent process for location information.** Create a clear, strong process with heightened standards for government access to information regarding the location of an individual's mobile device.

Advances in technology rely not just on the smart engineers who create the new services, but also on smart laws that provide the critical legal underpinning for continued innovation and adoption of the technology. We hope to work with this Committee and with Congress as a whole to strengthen these legal protections for individuals and businesses.

* * *

I look forward to answering any questions you might have about our efforts. And Google looks forward to working with members of the Committee and with Congress in the development of valuable online services and strong privacy and security protections for users.

Thank you.