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

Before the U.S. Senate Committee on Commerce, Science and Transportation
Subcommittee on Consumer Protection, Product Safety, and Insurance
"Consumer Privacy and Protection in the Mobile Marketplace"

May 19, 2011

Chairman Pryor, Ranking Member, 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 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 more than 170 devices today, created by 27 manufacturers. We also offer dozens of other popular services, from YouTube to Gmail to Google Earth.

Our business depends on protecting the privacy and security of our users. Without the trust of our users, they will simply switch to competing services, which are always just one click away. For this reason, location sharing on Android devices is strictly opt-in for our users, with clear notice and control. This is the way these services *should* work — with opt-in consent and clear, transparent practices, so consumers can make informed decisions about the location-based services that are so popular.

This is also why we are educating parents and children about online safety, and working with groups like ConnectSafely and Common Sense Media to address the important issues of digital literacy and citizenship, including how to use Google's privacy, security, and family safety tools.
In my testimony today, I'll focus on three main points:

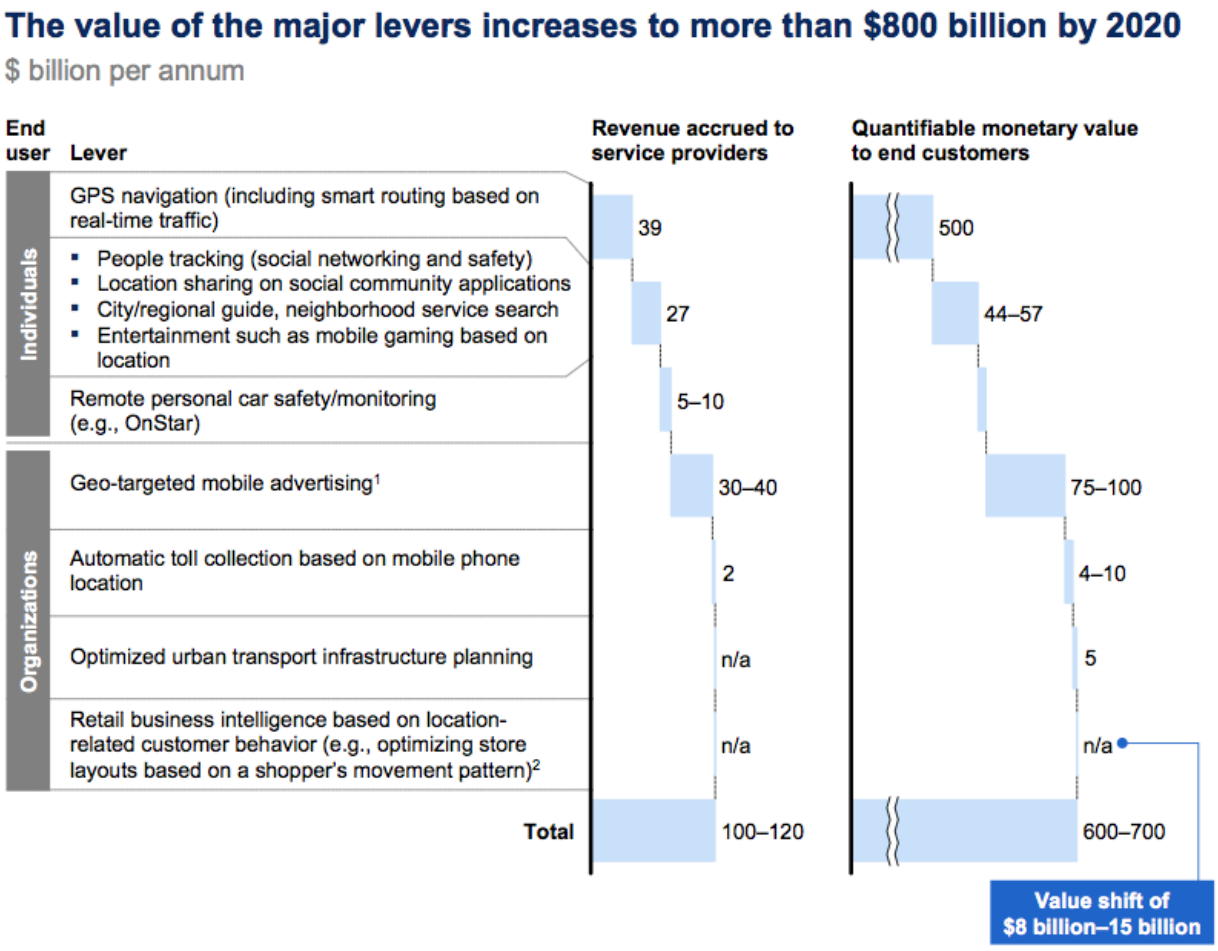
- Location-based services provide tremendous consumer benefit;
- Google is committed to the highest standards of privacy protection in our services, as demonstrated in our approach to mobile services, content controls, consumer education, advertising, and security; and
- Congress has an important role in helping companies build trust and create appropriate baseline standards for online privacy and security.

I. Location based services provide tremendous value to consumers

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. McKinsey estimates that personal location applications will generate as much as $700 billion in consumer value in the next eight years.

People can use mobile services to get driving directions from their current location, identify a traffic jam and find an alternate route, and look up 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 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.

Thousands of other organizations and entrepreneurs offer applications that 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. If you want a Five Guys burger, their application will find a location for you, and even lets you order in advance. Services such as Yelp and Urbanspoon use location to provide local search results, while applications like Foursquare let users find nearby friends who have chosen to share their location.



Source: McKinsey Global Institute analysis

Mobile location data can even save lives. In crisis situations, people now turn to the Internet to find information. Within a few hours of the Japan earthquake, for example, Google 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 announcements across Google 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.

Other emergency notifications like AMBER alerts can be improved using location data, too. In the past, a parent's best hope of finding a missing child might have been a picture on a milk carton. 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 through location-based targeting — within seconds of the first report, an AMBER alert could be distributed to all users within one-mile of the incident. As Ernie

Allen, NCMEC's President and CEO, wrote last week:

> Google's contributions to our Missing Child Division have also been significant. Your tools and specialized engineering solutions assist our case managers in the search for missing children. . . . We eagerly await the completed development of the AMBER Alert tool, which will expand the reach and distribution of AMBER alerts to Google users and will surely have enormous potential for widespread dissemination of news about serious child abduction cases. Thank you for your continued efforts to give children the safer lives that they deserve.

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 that help businesses and governments effectively reach their audiences.

II. Google is committed to the highest standards of privacy protection in our services

Google would not be able to offer these services — or help create the economic and social value generated from location data — if we lost the trust of our users. 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.

Our privacy principles

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.

First, 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. **We never sell our users' personally identifiable information**. This is simply not our business model.

Second, 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 lay out our substantive approach to privacy: We are committed to *transparency*, *user control,* and *security*.

Internal process and controls

Google also reflects these principles in our development process and employee training. As we recently explained, we have begun to implement even stronger internal privacy controls with a focus on people, training, and compliance.

All this process is aimed at ensuring that products match our philosophy and avoid mistakes that jeopardize user trust — like the launch of Google Buzz, which fell 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 our privacy procedures every two years. In addition, we'll ask users to give us affirmative consent before we change how we share their personal information.

Products reflecting principles: Opt-in location controls on Android

We understand location information is sensitive. So our approach to location data is simple: Opt-in consent and clear notice are required for collection and use of location information on Android.

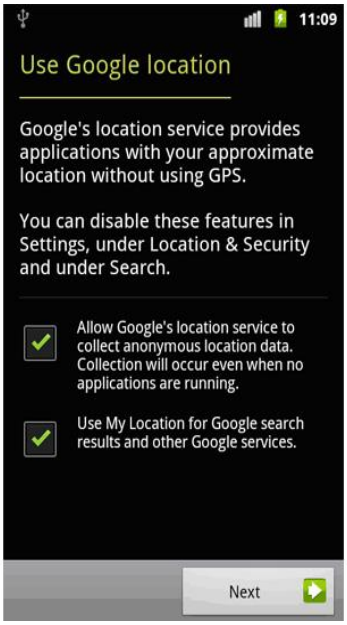
We don't collect any location information — any at all — through our location services on Android devices unless the user specifically chooses to share this information with Google. We also give users clear notice and control; the set-up process explicitly asks users to "allow Google's location service to collect anonymous location data." And even after the set-up process, users can 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. We hope that this will be a standard for the industry.

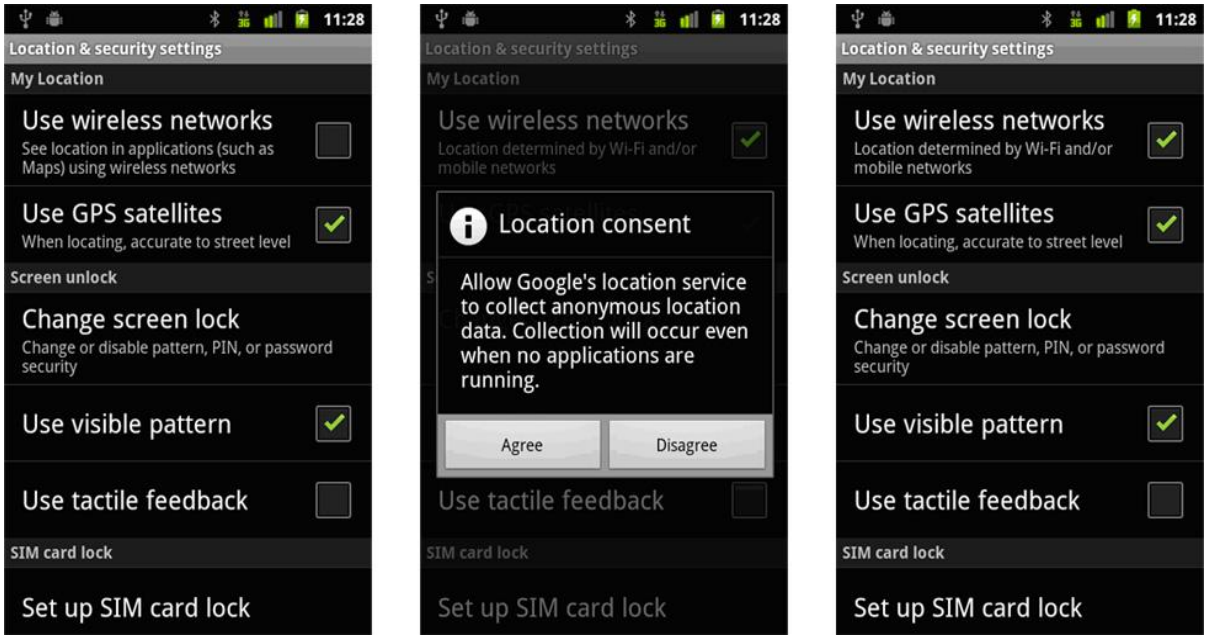
Google is also very careful about how we use and store the data that is generated by these services. The location information sent to Google servers when users opt in to location services on Android is anonymized and stored in the aggregate. It's not tied or traceable to a specific user. The collected information is stored with a hashed version of an anonymous token, and that hashed token 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.

In order to provide these location services, many companies detect nearby, publicly available signals from Wi-Fi access points and cell towers and use this data to quickly approximate a rough position, 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). Companies like Skyhook Wireless and Navizon compile such information and license the data to many industry leaders.

Google has a similar location service called the Google Location Server — an Internet database 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 license the Network Location Provider application for Android from Google. This Network Location Provider is turned off by default. It can be turned on by the user during the phone's initial setup or in the device settings.



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



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 openness, with the goal of encouraging developers to innovate. 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. 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 notice for this permission to the user at time of installation.

When Google creates an Android application, like Google Maps for mobile devices, Google is responsible for how the application collects and handles data and for the privacy disclosures made to users, and generally applies the Google Mobile Terms of Service and the Google Mobile Privacy Policy. These 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 its design and its use of data. Google does not and cannot 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. Google does strongly encourage application developers to use best practices as described in this Google blog post.

How our products reflect our principles: Parental controls and family safety

While Google does not offer services directed at children, we try to provide families with the tools and education to ensure a positive and safe experience on our services. In addition to our work with NCMEC and others to protect children, our major consumer education initiatives include:

- **Android Market content ratings.** The content rating system is a new feature of Android Market that requires developers to rate their apps in one of four categories, in accordance with our guidelines: Everyone, Low-, Medium-, or High-Maturity. Developers are responsible for rating the apps, and if users come across incorrectly rated apps, they can flag them for review.

- **SafeSearch on Mobile**. Just as with Google Web Search on desktop, Google's SafeSearch filter is accessible on mobile for users who search on a mobile browser. SafeSearch uses advanced technology to block sexually explicit images and text from search results. Users can customize and lock their SafeSearch settings to 'Strict' or 'Moderate' by clicking on the 'Settings' link to the top right corner of the homepage on Google.com.

- **Digital Literacy initiative.** To help educate families about responsible Internet use, we developed a curriculum with iKeepSafe that teaches teens to recognize online risks, investigate and determine the reliability of websites, and avoid scams. We've sponsored a tour that iKeepSafe is taking across the country to bring the curriculum into local communities and classrooms.

- **Family Safety Center.** In cooperation with the Federal Trade Commission's OnGuardOnline initiative and other child safety advocates and experts, we built a one-stop shop for families, available at www.google.com/familysafety, to provide step-by-step instructions for using safety tools built into Google products and other best practices for families to consider. In response to popular requests, we've added a section about managing geolocation features on mobile phones.

- **Net Safety Tips on the Go app.** The Internet Education Foundation, in partnership with Google and others, created an app to help users keep up with online privacy, safety, and security issues on your Android phone. It provides quick, practical, friendly advice for you and your family. The tips,

developed by leading online safety organizations, cover important issues like mobile privacy and safety, sexting and cyberbullying, social networking safety, and avoiding identity theft.

How our products reflect our principles: Advertising and privacy

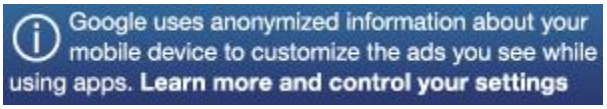
John Wanamaker, considered by some to be the father of modern advertising, once remarked that "half the money I spend on advertising is wasted; the trouble is I don't know which half." Google's advertising products are aimed at eliminating that wasted half, bringing data-driven efficiency to advertising. But as we work to bring more relevant and useful ads to our users, we continually seek to preserve transparency and user control over the information used in our ad system.

Google was not the first to offer interest-based advertising (known as IBA) online, but when we launched IBA, in March 2009, we included a number of groundbreaking privacy features. Google's interest-based ads contain notice in the actual advertisement indicating that it is a Google ad. The in-ad notice is linked to information about IBA, including our Ads Preferences Manager, which allows users to change the interest categories used to target ads, or to opt-out of interest-based advertising altogether. Note that we do not serve interest-based ads based on sensitive interest categories such as health status or categories relating to kids. We are also participating in the industry-wide ad targeting notice and opt-out program.

We have seen that for every visitor that opts out of IBA on this page, seven users view or edit their settings and choose to remain opted in. We take from this that online users appreciate transparency and control, and become more comfortable with data collection and use when we offer it on their terms and in full view.

Recently, discussions about online ad targeting have centered on the ability of users to indicate a desire to opt out of this profiling and targeting by all online providers — sometimes called Do Not Track. In January, Google sought to further encourage consistency and ease of control over online targeting by launching the Keep My Opt-Outs Chrome extension, which enables all providers participating in ever-expanding industry self-regulatory programs to make their IBA opt outs *permanent* via a simple browser-based mechanism. As new opt outs come online, we will automatically update this extension to keep users up to date. In the first few months, more than 100,000 users have already installed and are using the extension. We even released this tool on an open-source basis so that other developers can examine, assess, enhance, or even extend the code's capabilities. Additionally, we are developing versions of Keep My Opt Outs that work on other major browsers.

Just last month, we extended our advertising privacy approach to our mobile application ad networks. These networks help mobile app developers make money from their products. For these ad systems, we have created a user-friendly solution involving anonymization, user control, and user notice. First, Google performs a one-way, non-reversible hashing of a device identifier to create an anonymous ID specifically for ad serving. Second, for both Android and iPhone users we give consumers an easy way to opt out the use of their device identifier by Google's advertising services altogether. Third, we are notifing all users of how we customize ads and their opt-out controls with clear notice as you see here.



Because the mobile application interfaces are more limited, we chose to rotate full-size privacy notices in with other advertisements, rather than use an icon, which is hard to see or click on the smaller mobile screen.

How our products reflect our principles: Security through 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.

For example, Google was the first (and still 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 used for online banking and other secure transactions. Users can also encrypt search. Just type "https://encrypted.google.com" into your browser to encrypt your search queries and results. We hope other companies will soon join our lead.

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 herself and her contacts.

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 baseline standards

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

The first step Congress can take, and one on which we can all find common ground, is the need for basic "digital citizenship" education for parents, children, teens, and all consumers. Digital skills are essential life skills in a 21st century economy, including understanding basic technical concepts like how to create a safe password and avoid online scams, to critical thinking such as evaluating whether information on a blog is reliable or not. It is crucial that Congress and providers work together to create resources for programs that address these issues and promote them to all consumers, particularly parents and educators.

A second area for careful consideration is legislation. Google supports the development of comprehensive, baseline privacy framework that can ensure broad-based user trust and that will support continued innovation. We salute the work of Senators Kerry and McCain to develop a comprehensive approach to this issue, based on the same principles of transparency, control, and security we apply to our own services. We look forward to continued conversations about this bill as it evolves.

Key considerations for any comprehensive approach to privacy 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 privacy protocols would actually diminish consumer privacy, since it would require Internet companies to know where consumers are located at any given time.

By the same token, in general we do not support a continued "siloed" approach to privacy law. While much of today's debate centers on location information and "Do Not Track" advertising privacy proposals, providers and consumers need a comprehensive approach that will set consistent, baseline principles for these issues and those to come in the future. Otherwise, this Committee and others will be returning term after term to address the latest new technology fad.

Moreover, industry response to the advertising privacy issue has been encouraging. In a few short months, all major browser companies have introduced new controls, and the advertising and online publishing industries have come together to announce uniform standards for notice and control over targeted ads.

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

Congress should promote uniform, reasonable security principles, including data breach notification procedures. 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 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.

In addition, 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 compelled access to 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 stronger process for compelled access to 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.

* * *

Google appreciates the efforts of this subcommittee to address the critical privacy and security issues facing consumers. We look forward to working with you, and to answering any questions you might have about our efforts.

Thank you.