



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

Questions for the record from Senator Franken
Alan Davidson, Director of Public Policy, Google Inc.
June 8, 2011

1. Will Google commit to requiring that all apps in the Android Market have a clear, understandable privacy policy?

Google agrees that application developers that collect personal data from the users of their applications should offer clear notice of their practices, including via a privacy policy. Our Android Market developer agreement (<http://www.android.com/us/developer-distribution-agreement.html>) requires app developers to protect their users' privacy:

4.3 **You agree that if you use the Market to distribute Products, you will protect the privacy and legal rights of users.** If the users provide you with, or your Product accesses or uses, user names, passwords, or other login information or personal information, **you must make the users aware that the information will be available to your Product, and you must provide legally adequate privacy notice and protection for those users.** Further, your Product may only use that information for the limited purposes for which the user has given you permission to do so. If your Product stores personal or sensitive information provided by users, it must do so securely and only for as long as it is needed. . . .

(Emphasis added.)

Beyond privacy policies, we have also strongly encouraged developers to use best practices in the design of their applications as described in this Google blog post: <http://android-developers.blogspot.com/2010/08/best-practices-for-handling-android.html>.

Like the Federal Trade Commission and many others, we do not view privacy policies as the sole or even best way to provide clear notice of privacy practices. Unless a privacy policy is mandated by law, therefore, we have not *required* such a policy in order to satisfy the requirements of our developer agreement quoted above. We continue to evaluate this policy, and may revise it as needed to best protect the rights of Android users.

2. If not, will Google at least commit to require that all location-aware apps in the Android market have a clear, understandable privacy policy?

Please see the response to Question 1, above.

With respect to location information specifically, 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. The permissions model informs the user if an application will have access to the user's location information. An application can access the device's GPS location through a permission, which will display the permission message "Your location: fine (GPS) location" to the user during installation. An application can access the device's network location through a permission, which will display the permission message "Your location: coarse (network-based) location" to the user during installation.

3. Will Google commit to informing users through a clear, conspicuous method, i.e. a permission screen, that the apps they download have the technical ability to share or disclose the information they gather from the user to third parties?

As described above, we believe the permissions model provides clear, conspicuous notice to users about certain information that can be accessed by an application. An application can only send information off the device if it obtains Internet access. For an application to obtain Internet access, the user must grant a permission. Specifically, the user would see a permission message displayed saying: "Network communication: full Internet access" during installation.

The Android permissions model is designed to give users actionable information to help them decide whether to proceed with an application installation. The small size of a mobile device screen requires a delicate balance to determine the most useful quantity of information to present to the user. The downside of too little information is clear, but presenting too much information (especially if that additional information sounds like a legal disclaimer) could cause users to ignore the permission screen and defeat the goal of having better informed users.

One example of how we have recently adjusted this balance is demonstrated by our decision to show a longer permission description when a user installs an application from the web interface of Android Market (<http://market.android.com>) versus the on-device installation process. Users have the ability to browse applications on the large screen of their desktop or laptop computer through this website and push an installation of the application to their mobile device.

For example, the Android operating system will display a permission if an application wishes to access the device's GPS location. If the application installation is initiated from Android Market on the mobile device, the permission displayed on the phone says:

Your location: fine (GPS) location

This is a concise description appropriate for the small mobile device screen. If the application installation is initiated from Android Market through the web interface, the permission displayed on the website says:

YOUR LOCATION: FINE (GPS) LOCATION—Access fine location sources such as the Global Positioning System on the device, where available. Malicious applications can use this to determine where you are, and may consume additional battery power.

This is a more detailed description that takes advantage of the larger screen.

We will continue to consider ways to improve messaging to users, including with respect to this particular issue.

- 4. Do you think that most users understand the terms used in your app permission screen? For example, if an app can have access to your “network connections”, do you think the average user knows what that means? What can you do to make your permission screen more clear for average users without deep technical knowledge or sophistication?**

Please see our answer to Question #3 above. We have done our best to strike balances in our permissions model to make it understandable and useful in a way that benefits the maximum number users. We will continue to consider ways to improve the existing permission model.

- 5. Android OS devices transmit a unique identifier along with the location data that they transmit to Google servers. See Jennifer Valentino-Davies, “The Unique ID Android Uses in Collecting Location,” *The Wall Street Journal*, April 26, 2011. Apple succeeds in collecting this information without such an identifier. Will Google refrain from using such identifier in future data collection?**

We believe this identifier (which we refer to as an “anonymous token”) serves an important functional purpose, and have designed our systems in a way to protect user privacy.

The Google Network Location Provider application for Android (or NLP) is a proprietary Google application that may be installed on Android devices by a device manufacturer pursuant to a license with Google. NLP interacts with the Google Location Server (or GLS) to determine a user’s estimated location using Wi-Fi access points and cell towers, providing location information in a way that works indoors and outdoors, responds faster, and uses less battery power than GPS services.

With the opt-in consent of the user, NLP transmits certain location information to Google servers in association with an anonymous token randomly generated by GLS. A new token will be generated by GLS if the user performs a factory reset of the device. This token is only used to tag communications between NLP and GLS, which enables Google to compute velocity for road traffic estimates and to identify invalid transmissions to GLS. Google wants only legitimate devices to provide information, because invalid transmissions have the potential to pollute the GLS database with inaccurate data and degrade the ability of GLS to provide reliable location information to future users.

The collected information is stored in temporary databases on Google servers for approximately one week in association with a hashed version of the anonymous token. The token is put through a one-way hash as soon as it arrives at the server. The token itself is never stored on a Google server, only a hash of the token is temporarily stored in which the hash key is rotated at least every seven days. After this approximately one week of temporary storage, the information related to the hashed token values is stripped from the data and measures are taken to obfuscate GPS route endpoints. The remaining data is transferred into aggregate and anonymous databases on Google servers for permanent

storage, consisting of a database of Wi-Fi access point and cell tower locations and a database of road traffic information.

The design choice to use this anonymous token (rather than some other identifier) helps ensure that the information cannot be traced back to a particular device or particular user. Additional practices such as only storing a hashed version of the anonymous token, rotating the hash key, stripping the hashed token values, and taking measures to obfuscate GPS route endpoints are additional security measures instituted to further anonymize this information. Access by Google employees to the temporary and permanent databases is subject to access restriction policies and processes.

6. Under what circumstances does Google consider location information obtained from a user's device to be non-content customer records data subject to the voluntary disclosure permission in the Electronic Communications Privacy Act, 18 U.S.C. § 2702(c)(6)?

Without commenting on the specific legal question, we note that the location information sent to Google servers when users opt in to location services on Android devices is anonymized and stored in the aggregate and is not tied or traceable to a specific user. Therefore, Google cannot identify a particular user from the location information stored in our location servers and cannot produce information about a particular user.

7. Since Google gets the vast majority of its revenue from advertising, it seems like your incentive to protect privacy might be in conflict with your incentive to collect your user's information. What relationship does AdMob have to the Android Operating System and applications in the Android App Market?

The Android operating system and Android Market are part of one business unit, while AdMob is part of a separate unit. The AdMob product is not part of the Android operating system.

We note that offering free, advertising-supported services is not inherently in conflict with strong incentives to protect privacy. Many long-standing industries are advertising-supported, including broadcast television and newspapers, yet these businesses have little history of mistreatment of user privacy. Like providers of those services, our users are our lifeblood—without their trust and engagement, we would not have an audience to which to show ads.

Moreover, all businesses, regardless of their profit model, have an incentive to sell customer data—indeed, this path is followed by countless merchants, grocery chains, and even government agencies. Yet Google does not; we never sell our users' personally-identifiable information, or share it without their express consent.

Instead, we follow the axiom of “focus on the user and all else will follow.” This applies to every aspect of our business, including our treatment of personal information. As our testimony explains, Google would simply go out of business if we lost the trust of our users. This is reflected foremost in our privacy principles, which are located and available to the public at www.google.com/corporate/privacy_principles.html. Our commitment to these principles is reflected in our industry-leading privacy practices and tools, including our Ads Preferences Manager (<http://www.google.com/ads/preferences/>).