



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 Dr. Coburn
Alan Davidson, Director of Public Policy, Google Inc.
June 8, 2011

1. **Google has stated it does not sell users’ personally identifiable information to third parties. However, Google operates advertising services that are connected to mobile devices using its Android platform. Could you comment on how Google operates its ad services, particularly whether Google sends targeted ads to mobile device users, and if so, what user information Google collects in order to send targeted ads?**

Advertisers may use Google’s advertising services to run mobile advertising campaigns based on several factors. Those factors can include platform, device, geography, or demographic information.

To protect user privacy, Google adheres to the following principles when offering its advertising services and targeting options:

- **Transparency** – We provide detailed information about our advertising policies and practices (see our [general Google privacy policy](#) and [the AdMob privacy policy](#)).
- **Choice** – We offer innovative ways to view, manage and opt out of targeted advertising.
- **No personally identifying information** – We do not collect or serve ads based on personally identifying information without the user’s permission.

Recently, we extended our online advertising transparency and choice approach to our mobile application ad networks. 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 cryptographic hash of a device identifier which we then associate with 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 notifying all users of how we customize ads and their opt-out controls with clear notice. Because the mobile application interfaces are more limited, we chose to show a full-size privacy notice that was rotated along with other advertisements, rather than use an icon, which is hard to see or click on the smaller mobile screen.

- a. Is advertising the largest source of revenue for Google? If not, what services or products contribute most to Google's bottom line?**

Yes.

- b. Are there any apps to which Google refuses to provide advertising services? If so, what are the primary reasons for refusing such services? If not, why?**

Developers of mobile applications that use Google's advertising service (known as AdMob or AdSense for Mobile Apps) must agree to either AdMob's Terms of Use (<http://www.admob.com/home/terms>) and Publisher Guidelines and Policies (<http://helpcenter.admob.com/content/content-guidelines>), or AdSense's Terms of Use (<https://www.google.com/adsense/localized-terms>) and Publisher Guidelines and Policies (<https://www.google.com/adsense/support/bin/answer.py?answer=48182>).

If Google determines that a developer is in violation of these terms or policies, Google may take enforcement action. Depending on the severity of the violation, the enforcement action may take the form of a warning, suspension, or permanent termination.

- c. Are there any apps Google refuses to host on the Android app store? If so, what are the primary reasons for refusing to provide those apps, and how often, on average, does Google reject an app or later remove it from your store for questionable behavior?**

Google may suspend an application from future availability on Android Market if Google discovers that an application violates the Android Market developer agreement (<http://www.android.com/us/developer-distribution-agreement.html>) or policies (<http://www.android.com/us/developer-content-policy.html>). In addition to suspending an application, Google may also permanently disable the account of a developer for repeated or egregious violations of the Android Market developer agreement or policies.

Android Market is built on the principle of openness, with the goal of encouraging innovation and user choice. With this principle in mind, Google does not pre-screen applications before they are made available by developers to users of Android Market. But we will remove applications when we are notified about or otherwise discover applications that violate our developer agreement or policies. As of May 31, 2011, Google is removing an average of 250-300 applications per day from Android Market due to violations of our developer agreement or policies.

- d. How many employees and/or automated services are dedicated to crawling your app store to weed out apps that inappropriately use consumers' personal information or violate your respective privacy policies?**

We have a team of employees dedicated to responding to complaints and information we receive about applications in the Android Market to determine if the applications comply with our developer agreement and policies, but not specifically related to inappropriate use

of personal information. The size of this team is growing and will be adjusted as needed. Separately, we have recently implemented tools that automatically examine the code of Android Market applications for signs of potential malware.

More broadly, 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. 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 decisions about 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.

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. Even though the developer bears the responsibility, Google strongly encourages application developers to use best practices, as described in this Google blog post: <http://android-developers.blogspot.com/2010/08/best-practices-for-handling-android.html>.

Furthermore, developers that upload applications to Android Market must agree to the Android Market developer agreement (<http://www.android.com/us/developer-distribution-agreement.html>), pursuant to which developers agree to comply with applicable laws and to protect the privacy rights of users.

The specific relevant language is as follows:

4.2 You agree to use the Market only for purposes that are permitted by (a) this Agreement and (b) any applicable law, regulation or generally accepted practices or guidelines in the relevant jurisdictions (including any laws regarding the export of data or software to and from the United States or other relevant countries).

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. But if the user has opted into a separate agreement with you that allows you or your Product to store or use personal or sensitive information directly related to your Product (not including other products or applications) then the terms of that separate agreement will govern your use of such information. If the user provides your Product with Google Account information, your Product may only use that information to access the user's Google Account when, and for the limited purposes for which, the user has given you permission to do so.

- e. In other contexts, such as the sale of counterfeit pharmaceuticals online, there has been a recent push in the industry (with the suggestion of the Intellectual Property Enforcement Coordinator) to form a working group in order for the industry to take the lead on how to combat the dangerous use of these products online. Is there any such industry working group to address the unique issues surrounding mobile device products and/or location based services?**

There are numerous industry groups that address issues surrounding mobile device products and location based services. For example, CTIA - The Wireless Association publishes Best Practices and Guidelines for Location Based Services, available at: http://www.ctia.org/business_resources/wic/index.cfm/AID/11300. The Guidelines state that they are intended to promote and protect user privacy as new Location-Based Services ("LBS") are developed and deployed. As CTIA explains it, "Location Based Services have one thing in common regardless of the underlying technology – they rely on, use or incorporate the location of a device to provide or enhance a service. Accordingly, the guidelines are technology-neutral and apply regardless of the technology or mobile device used or the business model employed to provide LBS (e.g., a downloaded application, a web-based service, etc.)." Google supported the development of these guidelines.

Google also is a member of the Mobile Marketing Association, which represents more than 700 member companies globally. Its mission is to provide education, measurement and guidance to the mobile marketing industry worldwide. MMA has a standing committee on privacy and data security.

The Digital Advertising Alliance, composed of the bulk of the online advertising and publishing industry, has issued [guidelines for online behavioral advertising](#). They are working now to extend these guidelines into the mobile advertising area.

There are many other organizations and industry working groups that focus on particular aspects of the mobile industry and mobile devices.