Google and Mobile Privacy

Mobile devices offer users a new and different way to access Google products and services, but our approach to protecting privacy is consistent whether you're on a computer or on a cell phone. While our mobile products use parallel infrastructure, such as separate servers, the information we collect is essentially the same (with a few exceptions that we've created to make our mobile products work properly--for example, logs for mobile location-based services).

This information comes in two forms:

- **Authenticated account information** is the data tied to a Google Account that is collected when users are logged in to services like Gmail.
- **Unauthenticated information** is the data collected on services such as web search when users are not logged in with their username and password. This data is stored either as anonymous, aggregate information or with a random session ID number assigned to it. It's stored separately from Google Account information.

How we're protecting the privacy of mobile users

- **Transparency and User Control:** We tell users what information we store when they use our mobile services and make it easy for them to opt in or opt out of certain products, features, or data collection at any time by changing their privacy settings or choosing not to use particular features. Users also choose what information they share with other users and how they share it.
- **Protecting users' information:** We build our mobile services with privacy in mind and have policies that keep users' information private and secure.
    - Using a Google mobile service or the Android operating system does not mean that we know a user's phone number or have access to their calls or text messages. We only record a user's phone number when the user sends it to us (as in Send to Phone), asks us to remember it (as in Latitude), or makes a call or sends a text message to or from a Google service (as in Goog-411 or Google SMS). Similarly, we only have access to the content of users' phone calls or text messages when they call or text a Google service (as in Goog-411 or Google SMS).
    - We store unauthenticated information--such as logged-out searches, location info, and crash reports--separately from users' personal Google Account information.
    - The mobile IP addresses we receive from mobile carriers do not identify individual phones.

Google Voice Search

To make improvements to our voice search service, we store the audio files of user searches with a random session ID number which is anonymized after a short time. Since our voice recognition technology translates a voice search into a text search on Google, we also store a server log of every search just like we do with any query on Google.com from a computer or mobile phone. Users can turn voice search on or off in their settings at any time.

Location

Policies and practices vary by product, but we use protections such as opt-ins and privacy controls to keep our users' location information private and under their control. Many of Google's location-enabled services that use cell tower ID, Wi-Fi, or GPS information to approximate location--such as Search with My Location, Latitude, and the Google Gears Geolocation API--are opt-in; we tell users what information we're collecting, and they can turn the location feature on or off at any time. If a user does not use these location-enabled services, Google does not receive any data that can be used to approximate their phone's location. Users can also turn off GPS or Wi-Fi directly on their device at any time. Unauthenticated location information is stored separately from users' personal Google Account information.

Advertising

We show ads on mobile phones similarly to the desktop--using keywords and context on a web page. Ad cookies work the same way as they do on the desktop. Also, to show ads based on general geographic area, as on the desktop, we primarily use IP addresses. However, on a limited number of phones such as those that use Google's My Location feature, we may also serve ads based on more precise location signals derived from cell tower ID, Wi-Fi, or GPS only if the user consents to the use of their location information. Users can turn off My Location at any time. We don't share users' location information with advertisers, and location information for advertising purposes is not tied to a user's Google Account.

Android

Google does not collect additional information from cell phones that use the Android operating system beyond what we typically collect when someone uses Google products and services from their phone or desktop. The only exceptions are when wireless carriers partner directly with Google to release a phone that uses Android, such as the T-Mobile G1. In these cases:

- Google collects anonymous location information based on Wi-Fi scans in order to improve the quality of location-based services. We collect this information, which does not identify individual users, in aggregate form, and users can opt out of this at any time by disabling Wi-Fi.
- Google collects anonymous performance-related usage information such as the software version being used and the number of crashes experienced. These statistics do not involve personal information such as the content of messages or phone calls and are not associated with any user-specific information such as a user's Google Account or hardware ID number. Google analyzes these statistics in aggregate form in order to improve the Android software and user experience.

Android is open source, so anyone can build a phone that uses the Android operating system without partnering with Google. In these cases, this additional data is not collected from users.

The T-Mobile G1, in particular, asks users to log in to their Google Account. This login authenticates users in Google Mobile Services, which syncs users' account information so that they can easily access and use their Gmail, Google Calendar, Contacts, Google Talk instant messages, and other account information from their phone. However, logging in to a Google Account on the G1 does not mean that Google logs everything the user does on the G1. Instead, Google collects data as usual only when a device accesses Google services, just like from the desktop or any other phone, and for the cases mentioned above. Also, logging in to a Google Account on the G1 does not authenticate users across all Google services. A user's web searches, for example, remain unauthenticated unless users log in separately.

www.google.com 1600 Amphitheatre Parkway, Mountain View, CA 94043