

Testimony of Dr. Guy "Bud" Tribble
Vice President for Software Technology
Apple Inc.



On

Protecting Mobile Privacy:
Your Smartphones, Tablets, Cell Phones and Your Privacy

Before the

Subcommittee on Privacy, Technology and The Law
Committee on the Judiciary
United States Senate
Washington, DC

May 10, 2011

Good morning Chairman Franken, Ranking Member Coburn, and Members of the Subcommittee. My name is Bud Tribble, and I am Vice President for Software Technology for Apple Inc. On behalf of Apple, I thank you for the opportunity to address this important subject.

Apple's Commitment To Protecting Our Customers' Privacy

Apple is deeply committed to protecting the privacy of our customers who use Apple mobile devices, including iPhone, iPad and iPod touch. Apple has adopted a comprehensive privacy policy for all its products and implemented industry-leading privacy features in its products to protect our customers' personal data. We are also deeply committed to meeting our customers' demands for prompt and accurate location-based services. These services offer many benefits to our customers by enhancing convenience and safety for shopping, travel and other activities.

To meet these goals, Apple provides easy-to-use tools that allow our consumers to control the collection and use of location data on all our mobile devices. We do not share personally identifiable information with third parties for their marketing purposes without consent, and we require third-party application developers to agree to specific restrictions protecting our customers' privacy. Apple is constantly innovating new technology, features and designs to provide our customers with greater privacy protection and the best possible user experience.

Apple welcomes inquiries about how it protects its customers' privacy while providing reliable and fast location-based services. For instance, Apple provided on July 12, 2010 to Representatives Barton and Markey a detailed description of its collection and use of location-based information. I testified regarding the same topic before the Committee on Commerce, Science, and Transportation on July 27, 2010. And on April 27, 2011, Apple released a public response to recent questions regarding the collection and use of location information. A copy of that response is attached to this testimony as Exhibit A. The initial point made in that response should be emphasized: Apple does not track users' locations – Apple has never done so and has no plans to ever do so.

In my testimony today, I would like to address the following topics: (1) Apple's Privacy Policy; (2) Apple's collection, storage and use of location information on Apple mobile devices; and (3) the use of location information by third-party applications and the iAd Advertising Network.

I. Apple's Privacy Policy

Apple has a single Customer Privacy Policy (the "Policy") that applies across all Apple businesses and products, including the iTunes Store and App Store. The Policy, written in easy-to-read language, details what information Apple collects and how Apple and its partners and licensees may use the information. The Policy is available from a link on every page of Apple's website.¹

The Policy includes the following provision regarding location-based information:

To provide location-based services on Apple products, Apple and our partners and licensees may collect, use, and share precise location data, including the real-time geographic location of your Apple computer or device. This location data is collected anonymously in a form that does not personally identify you and is used by Apple and our partners and licensees to provide and improve location-based products and services. For example, we may share geographic location with application providers when you opt in to their location services.

Some location-based services offered by Apple, such as the MobileMe "Find My iPhone" feature, require your personal information for the feature to work.

This provision incorporates similar language regarding location-based information that appears in Apple End User Software License Agreements ("SLAs") for products that provide location-based services. For example, the current iPhone SLA states:

Apple and its partners and licensees may provide certain services through your iPhone that rely upon location information. To provide and improve these services, where available, Apple and its partners and licensees may transmit, collect, maintain, process and use your location data, including the real-time geographic location of your iPhone, and location search queries. The location data and queries collected by Apple are collected in a form that does not personally identify you and may be used by Apple and its partners and licensees to provide and improve location-based products and services. **By using any location-based services on your iPhone, you agree and consent to Apple's and its partners' and licensees' transmission, collection, maintenance, processing and use of your location data and queries to provide and improve such products and services.** (Emphasis exists in the SLA.) You may withdraw this consent at any time by going to the Location Services setting on your iPhone and either turning off the global Location Services setting or turning off the individual location settings of each location-aware application on your iPhone. Not using these location features will not impact the non location-based functionality of your iPhone. When using third party applications or services on the iPhone that use or provide location data, you are subject to and should review such

¹The links take customers to <http://www.apple.com/privacy>, which customers may also access directly.

third party's terms and privacy policy on use of location data by such third party applications or services.

The Policy includes the following provision regarding third-party products, such as iPhone apps:

Apple websites, products, applications, and services may contain links to third-party websites, products, and services. Our products and services may also use or offer products or services from third parties – for example, a third-party iPhone app. Information collected by third parties, which may include such things as location data or contact details, is governed by their privacy practices. We encourage you to learn about the privacy practices of those third parties.

The Policy also includes the following language regarding mobile advertisements, such as those served through Apple's iAd service:

Apple and its partners use cookies and other technologies in mobile advertising services to control the number of times you see a given ad, deliver ads that relate to your interests, and measure the effectiveness of ad campaigns. If you do not want to receive ads with this level of relevance on your mobile device, you can opt out by accessing the following link on your device: <http://oo.apple.com>. If you opt out, you will continue to receive the same number of mobile ads, but they may be less relevant because they will not be based on your interests. You may still see ads related to the content on a web page or in an application or based on other non-personal information. This opt-out applies only to Apple advertising services and does not affect interest-based advertising from other advertising networks.

The Policy identifies a dedicated page on Apple's website where customers may submit privacy-related inquiries and comments. Apple monitors these submissions and responds to appropriate inquiries in a timely manner. Customers may also address privacy concerns to TRUSTe, Apple's third-party privacy monitor. A link to TRUSTe is displayed within the Policy.

As noted above, customers may access the Policy from every page on Apple's website. The Policy also was placed where Apple believed the largest number of customers would see it: the iTunes Store.

Customers attempting to open a new iTunes Store account are directed to a webpage titled: "iTunes Store Terms & Conditions and Apple's Privacy Policy." They are asked to click the same unchecked agreement box stating: "I have read and agree to the iTunes Terms and Conditions and Apple's Privacy Policy."

Apple updated the Policy on June 21, 2010.² The first time each existing iTunes Store customer logged on to the iTunes Store after that date, the iTunes Store displayed a message that prompted the customer to review the iTunes Store Terms and Conditions. The message stated:

²Note that on March 31, 2011, Apple made two non-material updates to its June 21, 2010 Privacy Policy. Specifically, Apple updated: (1) the URL where users can login to their accounts to view and modify their preferences and contact information and (2) the mechanism provided to users to ask questions about the Policy.

iTunes Store Terms and Conditions have changed. Please read and agree to the terms and conditions below to continue using the iTunes Store.

Customers were asked to click an unchecked agreement box stating: "I have read and agree to the iTunes Terms and Conditions and Apple's Privacy Policy." Customers who do not agree to the Terms and Conditions and the Policy are not be able to use the iTunes Store (e.g., cannot make purchases on the iTunes Store or the App Store), but they may continue to use iTunes software.

II. Location Information and Location-Based Services for Mobile Devices

Apple began providing location-based services in January 2008. These services enable applications that allow customers to perform a wide variety of useful tasks such as getting directions to a particular address from their current location or finding nearby restaurants or stores.

Apple offers location-based services on a variety of mobile devices, including the iPhone 3G, iPhone 3GS, iPhone 4 CDMA and GSM models, iPad Wi-Fi + 3G, iPad 2 Wi-Fi and 3G and, to a more limited extent, older models of the iPhone, the iPad Wi-Fi, and iPod touch.

All of Apple's mobile devices run on Apple's proprietary mobile operating system, iOS. Apple released iOS 4.1 on September 8, 2010. Apple released the current versions, iOS 4.3.3 and 4.2.8 (for the iPhone 4 CDMA model), on May 4, 2011. Currently, iOS 4.3.3 may be run on iPhone 3GS, iPhone 4 GSM model, iPod touch 3rd and 4th generations, iPad, and iPad 2. My testimony focuses on iOS 4.1 and later versions, including the free iOS update Apple released on May 4, 2011.

A. Privacy Features


Apple has designed features that enable customers to exercise control over the use of location-based services.

First, Apple provides its customers with the ability to turn "Off" all location-based service capabilities with a single "On/Off" toggle switch. For mobile devices, the toggle switch is in the "Location Services" menu under "Settings." As described more fully below, when this toggle is switched "Off," (1) iOS will not provide any location information to any applications, including applications that may have previously received consent to use location information; (2) iOS will not collect or geo-tag information about nearby Wi-Fi hotspots or cell towers; and (3) iOS will not upload any location information to Apple from the device.

Second, Apple requires express customer consent when any application requests location-based information for the first time. When an application requests the information, a dialog box appears stating: "[Application] would like to use your current location." The customer is asked: "Don't Allow" or "OK." If the customer clicks on "Don't Allow," iOS will not provide any location-based information to the application. This dialog box is mandatory—neither Apple's applications nor those of third parties are permitted to override the notification.

Third, iOS 4 permits customers to identify individual applications that may not access location-based information, even if Location Services is "On." The Location Services settings menu

provides an “On/Off” toggle switch for each application that has requested location-based information. When the switch for a particular application is “Off,” no location-based information will be provided to that application.

Fourth, Customers can change their individual application settings at any time. An arrow icon () alerts iOS 4 users that an application is using or has recently used location-based information. This icon will appear real-time for currently running applications and next to the “On/Off” switch for any application that has used location-based information in the past twenty-four hours.

Finally, customers can use Restrictions, also known as Parental Controls, on a mobile device to prevent access to specific features, including Location Services. When a customer enables Restrictions, the customer must enter a passcode (this passcode is separate from the device passcode that the customer may set). If the customer turns Location Services off and selects “Don’t Allow Changes,” the user of the device cannot turn on Location Services without that passcode.

B. Location Information

1. Crowd-Sourced Database of Cell Tower Location and Wi-Fi Hotspot Information

Customers want and expect their mobile devices to be able to quickly and reliably determine their current locations in order to provide accurate location-based services. If the device contains a GPS chip, the device can determine its current location using GPS satellite data. But this process can take up to several minutes. Obviously, if the device does not have a GPS chip, no GPS location data will be available.

To provide the high quality products and services that its customers demand, Apple must have access to comprehensive location-based information. To enable Apple mobile devices to respond quickly (or at all, in the case of non-GPS equipped devices or when GPS is not available, such as indoors or in basements) to a customer’s request for current location information, Apple maintains a secure database containing information regarding known locations of cell towers and Wi-Fi access points – also referred to as Wi-Fi hotspots. As described in greater detail below, Apple collects from millions of Apple devices anonymous location information for cell towers and Wi-Fi hotspots.³ From this anonymous information, Apple has been able, over time, to calculate the known locations of many millions of Wi-Fi hotspots and cell towers. Because the basis for this location information is the “crowd” of Apple devices, Apple refers to this as its “crowd-sourced” database.

The crowd-sourced database contains the following information:

Cell Tower Information: Apple collects information about nearby cell towers, such as the location of the tower(s), Cell IDs, and data about the strength of the signal transmitted from the towers. A Cell ID refers to the unique number assigned by a cellular provider to a cell, a defined geographic area covered by a cell tower in a

³ During this collection process, iOS does not transmit to Apple any data that is uniquely associated with the device or the customer.

mobile network. Cell IDs do not provide any personal information about mobile phone users located in the cell. Location, Cell ID, and signal strength information is available to anyone with certain commercially available software.

Wi-Fi Access Point Information: Apple collects information about nearby Wi-Fi access points, such as the location of the access point(s), Media Access Control (MAC) addresses, and data about the strength and speed of the signal transmitted by the access point(s). A MAC address (a term that does not refer to Apple products) is a unique number assigned by a manufacturer to a network adapter or network interface card ("NIC"). MAC addresses do not provide any personal information about the owner of the network adapter or NIC. Anyone with a wireless network adapter or NIC can identify the MAC address of a Wi-Fi access point. Apple does not collect the user-assigned name of the Wi-Fi access point (known as the "SSID," or service set identifier) or data being transmitted over the Wi-Fi network (known as "payload data").

The crowd-sourced database does not reveal personal information about any customer. An Apple mobile device running Apple's mobile device operating system, iOS, can use the crowd-sourced database to (1) provide the customer with an approximate location while waiting for the more precise GPS location, (2) find GPS satellites much more quickly, significantly reducing the wait time for the GPS location, and (3) triangulate the device location when GPS is not available (such as indoors or in basements). The device performs all of these calculations in response to a request for location information from an application on the customer's device that has been explicitly approved by the user to obtain the current location, and the device requests from Apple the crowd-sourced database information needed for these calculations.⁴

The crowd-sourced database must be updated continuously to account for, among other things, the ever-changing physical landscape, more innovative uses of mobile technology, and the increasing number of Apple's customers. In collecting and maintaining its crowd-sourced database, Apple always has taken great care to protect its customers' privacy.

2. Downloading Crowd-Sourced Data To A Mobile Device

To further improve the speed with which the device can calculate location, Apple downloads a subset of the crowd-sourced database content to a local cache on the device. This content describes the known locations of Wi-Fi hotspots⁵ and cell towers that the device can "see" and/or that are nearby, as well as nearby cell location area codes,⁶ some of which may be more than one hundred miles away. The presence of the local cache on the device enables

⁴For devices running the iPhone OS versions 1.1.3 to 3.1, Apple relied on (and still relies on) databases maintained by Google and Skyhook Wireless ("Skyhook") to provide location-based services. Beginning with the iPhone OS version 3.2 released in April 2010, Apple relies on its own databases to provide location-based services and for diagnostic purposes.

⁵For each Wi-Fi hotspot, the location information includes that hotspot's MAC address, latitude/longitude coordinates, and associated horizontal accuracy number. For each cell tower, the location information includes the cell tower ID, latitude/longitude coordinates, and associated horizontal accuracy number.

⁶Cell base stations are grouped into "location areas" for network planning purposes, and each location area is assigned a unique "location area code." This "location area code" is broadcast by the cell base stations.

the device to calculate an initial approximate location before Apple's servers can respond to a request for information from the crowd-sourced database.

The local cache does not include a log of each time the device was near a particular hotspot or cell tower, and the local cache has never included such a log. For each Wi-Fi hotspot and cell tower, the local cache stores only that hotspot's/cell tower's most recent location information, downloaded from Apple's constantly updated crowd-sourced database. After a customer installs the free iOS software update, iOS will purge records that are older than seven days, and the cache will be deleted entirely when Location Services is turned off.

The local cache is protected with iOS security features, but it is not encrypted. Beginning with the next major release of iOS, the operating system will encrypt any local cache of the hotspot and cell tower location information.

Apple issued a free iOS software update on May 4, 2011. Prior to the update, iTunes backed up the local cache (stored in consolidated.db) as part of the normal device backup if there was a syncing relationship between the device and a computer. The iTunes backup, including consolidated.db, may or may not have been encrypted, depending on the customer's settings in iTunes. After the software update, iTunes does not back up the local cache (now stored in cache.db).

When a customer runs certain applications, those applications request location information from iOS. Because of a bug that existed prior to the update, even when Location Services was off, the device would anonymously send the IDs of visible Wi-Fi hotspots and cell towers, without any GPS information, to Apple's servers, Apple's servers would send back the known, crowd-sourced location information for those hotspots and cell towers (and nearby hotspots and cell towers), and the device would cache that information in the consolidated.db file. None of this downloaded crowd-sourced location information – or any other location information – was provided to or disclosed to the application.

The iOS software update fixed the bug that caused crowd-sourced location information to be downloaded to the device while Location Services was off. iOS will now delete any existing local cache from consolidated.db and, if Location Services is off, (1) Apple will not download any crowd-sourced location information to the device, regardless of whether a specific application requests that information, and (2) iOS will delete any cache of this information stored in cache.db.

3. Collections and Transmissions from Apple Mobile Devices

Apple collects anonymous location information about Wi-Fi hotspots and cell towers from millions of devices to develop and refine Apple's database of crowd-sourced location information. The mobile devices intermittently collect information about Wi-Fi hotspots and cell towers they can "see" and tag that information with the device's current GPS coordinates, i.e. the devices "geo-tag" hotspots and towers.

This collected Wi-Fi hotspot and cell tower information is temporarily saved in a separate table in the local cache; thereafter, that data is extracted from the database, encrypted, and transmitted – anonymously – to Apple over a Wi-Fi connection every twelve hours (or later if the device does not have Wi-Fi access at that time). Apple's servers use this information to recalculate and update the known locations of Wi-Fi hotspots and cell towers stored in its crowd-sourced database. Apple cannot identify the source of this information, and Apple

collects and uses this information only to develop and improve the Wi-Fi hotspot and cell tower location information in Apple's crowd-sourced database. After the device attempts to upload this information to Apple, even if the attempt fails, the information is deleted from the local cache database on the device. In versions of iOS 4.1 or later, moreover, the device will not attempt to collect or upload this anonymous information to Apple unless Location Services is on and the customer has explicitly consented to at least one application's request to use location information.

4. Additional Location Information Collections

If Location Services is on, Apple collects location information from mobile devices under the following four additional circumstances.

First, as mentioned in Apple's April 27 response, Apple is collecting anonymous traffic data to build a crowd-sourced automobile traffic database with the goal of providing iPhone users an improved traffic service in the next couple of years. This information is temporarily stored in the local cache on the device, anonymously uploaded to Apple, and then deleted from the device.

Second, Apple collects anonymous diagnostic information from randomly-selected devices to evaluate and improve the performance of its mobile hardware and operating system. For example, Apple may collect information about a dropped cell phone call, including the calculated location of the device when a call was dropped, to help identify and address any cell connection issues. Before any diagnostic information is collected, the customer must provide express consent to Apple. Apple cannot associate this information with a particular customer.

Third, Apple obtains information about the device's location (the latitude/longitude coordinates) when an ad request is made. The device securely transmits this information to the Apple iAd servers, the iAd servers immediately convert the latitude/longitude coordinates to a five-digit zip code, and the iAd servers then discard the coordinates. Apple does not record or store the latitude/longitude coordinates – Apple stores only the zip code. Apple then uses the zip code to select a relevant ad for the customer.

Finally, if a customer has consented to an application's collection and/or use of location information, iOS will provide current location information in response to a request from that application. iOS will provide that customer-approved application with the location of the device only; iOS does not provide applications with direct access to the local cache.

III. Third-Party Applications And The iAd Network

A. Third Party Applications

In July 2008, Apple launched the App Store where customers may shop for and acquire applications offered by third-party developers for the iPhone, iPad and iPod touch. Currently the App Store includes more than 350,000 third-party applications covering a wide variety of areas including news, games, music, travel, health, fitness, education, business, sports, navigation and social networking. Each application includes a description prepared by the developer regarding, among other things, what the application does, when it was posted, and, if applicable, what information the application may collect from the customer.

Any customer with an iTunes account may purchase and download applications from the App Store. Developers do not receive any personal information about customers from Apple when applications are purchased. Only Apple has access to that information.

Third-party application developers must register as an “Apple Developer” by paying a fee and signing the iPhone Developer Agreement (the “IDA”) and the Program License Agreement (the “PLA”). Registered Apple Developers gain access to the software development kit (“SDK”) and other technical resources necessary to develop applications for mobile devices.

The current PLA contains several provisions governing the collection and use of location-based information, including the following:

- Developers may collect, use, or disclose to a third party location-based information only with the customer’s prior consent and to provide a service or function that is directly relevant to the use of the application;
- Developers must provide information to their customers regarding the use and disclosure of location-based information (e.g., a description on the App Store or adding a link to the applicable privacy policy);
- Developers must take appropriate steps to protect customers’ location-based information from unauthorized use or access;
- Developers must comply with applicable privacy and data collection laws and regulations regarding the use or transmission of location-based information;
- Applications must notify and obtain consent from each customer before location data is collected, transmitted, or otherwise used by developers;
- If the customer denies or withdraws consent, applications may not collect, transmit, process or utilize the customer’s location data; and
- Applications must not disable, override, or otherwise interfere with Apple-implemented alerts, including those intended to notify the customer that location-based information is being collected, transmitted, maintained, processed, or used, or intended to obtain consent for such use.

Developers that do not agree to these provisions may not offer applications on the App Store. Apple has the right to terminate the PLA if a developer fails to comply with any of these provisions.

Apple reviews all applications before adding them to the App Store to ensure, for example, that they run properly and do not contain malicious code. Apple, however, does not monitor applications after they are listed in the App Store, unless issues or problems arise.

B. The iAd Network

On July 1, 2010, Apple launched the iAd mobile advertising network. The network can serve ads to iPhone, iPod touch, and iPad devices running iOS 4, and the network offers a dynamic way to incorporate and access advertising within applications. Customers can receive advertising that relates to their interests (“interest-based advertising”) and/or their location

("location-based advertising"). For example, a customer who purchased an action movie on iTunes may receive advertising regarding a new action movie being released in the theaters or on DVD. A customer searching for nearby restaurants may receive advertising for stores in the area.

As specified in the Policy and the relevant device SLAs, customers may opt out of interest-based advertising by visiting the following site from their mobile device: <https://oo.apple.com>. Customers also may opt out of location-based advertising by toggling the device's location-based service capabilities to "Off."

For customers who do not toggle location-based service capabilities to "Off," Apple collects information about the device's location (latitude/longitude coordinates) when an ad request is made. This information is transmitted securely to the Apple iAd server via a cellular network connection or Wi-Fi Internet connection. The latitude/longitude coordinates are converted immediately by the server to a five-digit zip code. Apple does not record or store the latitude/longitude coordinates—Apple stores only the zip code. Apple then uses the zip code to select a relevant ad for the customer.

Apple does not share any interest-based or location-based information about individual customers, including the zip code calculated by the iAd server, with advertisers. Apple retains a record of each ad sent to a particular device in a separate iAd database, accessible only by Apple, to ensure that customers do not receive overly repetitive and/or duplicative ads and for administrative purposes.

In some cases, an advertiser may want to provide more specific information based on a device's actual location. For example, a retailer may want its ad to include the approximate distance to nearby stores. A dialog box will appear stating: "'Advertiser' would like to use your current location." The customer is presented with two options: "Don't Allow" or "OK." If a customer clicks "Don't Allow," no additional location information is transmitted. If the customer clicks "OK," Apple uses the latitude/longitude coordinates to provide the ad application with more specific location information—the information is not provided to the advertiser.

In closing, let me again affirm that Apple is strongly committed to protecting our customers' privacy. We give our customers clear notice of our privacy policies, and our mobile products enable our customers to exercise control over their personal information in a simple and elegant way. We share the Committee's concerns about the collection and potential misuse of all customer data, particularly personal information, and we appreciate this opportunity to explain our policies and procedures.

I will be happy to answer any questions you may have.

Exhibit A
April 27, 2011
Apple Q&A on Location Data

Mac
iPod
iPhone
iPad
iTunes
Support

April 27, 2011

Apple Q&A on Location Data

Apple would like to respond to the questions we have recently received about the gathering and use of location information by our devices.

1. Why is Apple tracking the location of my iPhone?

Apple is not tracking the location of your iPhone. Apple has never done so and has no plans to ever do so.

2. Then why is everyone so concerned about this?

Providing mobile users with fast and accurate location information while preserving their security and privacy has raised some very complex technical issues which are hard to communicate in a soundbite. Users are confused, partly because the creators of this new technology (including Apple) have not provided enough education about these issues to date.

3. Why is my iPhone logging my location?

The iPhone is not logging your location. Rather, it's maintaining a database of Wi-Fi hotspots and cell towers around your current location, some of which may be located more than one hundred miles away from your iPhone, to help your iPhone rapidly and accurately calculate its location when requested. Calculating a phone's location using just GPS satellite data can take up to several minutes. iPhone can reduce this time to just a few seconds by using Wi-Fi hotspot and cell tower data to quickly find GPS satellites, and even triangulate its location using just Wi-Fi hotspot and cell tower data when GPS is not available (such as indoors or in basements). These calculations are performed live on the iPhone using a crowd-sourced database of Wi-Fi hotspot and cell tower data that is generated by tens of millions of iPhones sending the geo-tagged locations of nearby Wi-Fi hotspots and cell towers in an anonymous and encrypted form to Apple.

4. Is this crowd-sourced database stored on the iPhone?

The entire crowd-sourced database is too big to store on an iPhone, so we download an appropriate subset (cache) onto each iPhone. This cache is protected but not encrypted, and is backed up in iTunes whenever you back up your iPhone. The backup is encrypted or not, depending on the user settings in iTunes. The location data that researchers are seeing on the iPhone is not the past or present location of the iPhone, but rather the locations of Wi-Fi hotspots and cell towers surrounding the iPhone's location, which can be more than one hundred miles away from the iPhone. We plan to cease backing up this cache in a software update coming soon (see Software Update section below).

5. Can Apple locate me based on my geo-tagged Wi-Fi hotspot and cell tower data?

No. This data is sent to Apple in an anonymous and encrypted form. Apple cannot identify the source of this data.

6. People have identified up to a year's worth of location data being stored on the iPhone. Why does my iPhone need so much data in order to assist it in finding my location today?

This data is not the iPhone's location data—it is a subset (cache) of the crowd-sourced Wi-Fi hotspot and cell tower database which is downloaded from Apple into the iPhone to assist the iPhone in rapidly and accurately calculating location. The reason the iPhone stores so much data is a bug we uncovered and plan to fix shortly (see Software Update section below). We don't think the iPhone needs to store more than seven days of this data.

7. When I turn off Location Services, why does my iPhone sometimes continue updating its Wi-Fi and cell tower data from Apple's crowd-sourced database?

It shouldn't. This is a bug, which we plan to fix shortly (see Software Update section below).

8. What other location data is Apple collecting from the iPhone besides crowd-sourced Wi-Fi hotspot and cell tower data?

Apple is now collecting anonymous traffic data to build a crowd-sourced traffic database with the goal of providing iPhone users an improved traffic service in the next couple of years.

9. Does Apple currently provide any data collected from iPhones to third parties?

We provide anonymous crash logs from users that have opted in to third-party developers to help them debug their apps. Our iAds advertising system can use location as a factor in targeting ads. Location is not shared with any third party or ad unless the user explicitly approves giving the current location to the current ad (for example, to request the ad locate the Target store nearest them).

10. Does Apple believe that personal information security and privacy are important?

Yes, we strongly do. For example, iPhone was the first to ask users to give their permission for each and every app that wanted to use location. Apple will continue to be one of the leaders in strengthening personal information security and privacy.

Software Update

Sometime in the next few weeks Apple will release a free iOS software update that:

- reduces the size of the crowd-sourced Wi-Fi hotspot and cell tower database cached on the iPhone,
- ceases backing up this cache, and
- deletes this cache entirely when Location Services is turned off.

In the next major iOS software release the cache will also be encrypted on the iPhone.

Press Contacts:

Natalie Harrison
Apple
harri@apple.com
(408) 862-0565

Natalie Kerris
Apple
nat@apple.com
(408) 974-6877

NOTE TO EDITORS: For additional information visit Apple's [PR website](#), or call Apple's Media Helpline at (408) 974-2042.

Apple, the Apple logo, Mac, Mac OS, Macintosh, iPhone and iTunes are trademarks of Apple. Other company and product names may be trademarks of their respective owners.