Testimony of Catherine A. Novelli
Vice President for Worldwide Government Affairs
Apple Inc.

On

Consumer Privacy and Protection in the Mobile Marketplace

Before the

Subcommittee on Consumer Protection, Product Safety and Insurance
Committee on Commerce, Science & Transportation
United States Senate
Washington, DC

May 19, 2011

Good morning Chairman Pryor, Ranking Member Wicker, and Members of the Subcommittee. My name is Catherine Novelli, and I am Vice President for Worldwide Government Affairs 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

As we stated in testimony provided before this Committee last summer, Apple is deeply committed to protecting the privacy of our customers who use Apple mobile devices, including iPhone, iPad and iPod touch.[1] Apple has adopted a single comprehensive privacy policy for all its businesses and products, including the iTunes Store and the App Store. Apple's Privacy 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.[2]

Apple takes security precautions – including administrative, technical, and physical measures – to safeguard our customers' personal information against loss, theft, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction. To make sure personal information remains secure, we communicate our privacy policy and security guidelines to Apple employees and strictly enforce privacy safeguards within the company.

We do not share personally identifiable information with third parties for their marketing purposes without consent. We require third-party application developers to agree to specific restrictions protecting our customers' privacy. Moreover, Apple's Safari browser is still the only browser to block cookies from third parties and advertisers by default.

---

[1] Testimony of Dr. Guy "Bud" Tribble of Apple Inc., on Consumer Online Privacy before the United States Senate Committee on Commerce, Science and Transportation, July 27, 2010.
[2] The links take customers to http://www.apple.com/privacy, which customers may also access directly.

As I will explain in more detail below, Apple is constantly innovating new technology, features and designs to provide our customers with greater privacy protection and the best possible user experience.

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. Apple does not track users' locations – Apple has never done so and has no plans to ever do so.

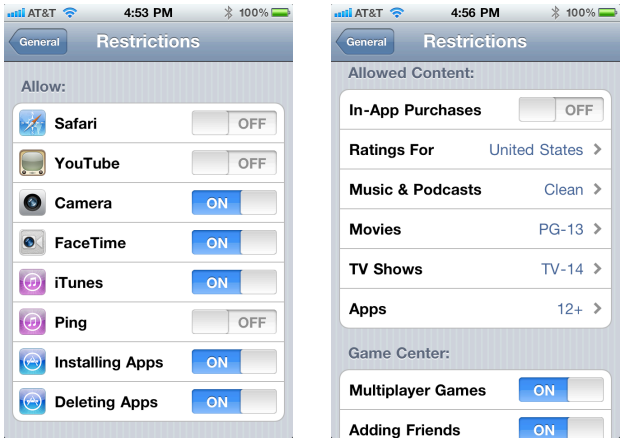
In my testimony today, I would like to reaffirm and amplify Apple's previous privacy testimony before this Committee, while focusing on the following topics of particular interest for this hearing: (1) Apple's Parental Controls and Restrictions settings; (2) Apple's collection, storage and use of location information on Apple mobile devices; and (3) the use of customer information by third-party applications and the iAd Advertising Network.

I. Apple's Parental Controls and Restrictions Settings

Apple has implemented industry-leading innovative settings and controls to enable parents to protect their children while using Apple products both on and off-line. These controls are easy to use, password protected, and can be administered on all Mac OS X products as well as on all of our iOS mobile devices, including iPhone, iPad and iPod Touch. These controls can also be enabled quite easily on the iTunes store.

On any Mac, parents can control which Apps their child can run as well as set age appropriate restrictions for the App Store. Parents also can control with whom their children can exchange emails or chat, where they can go online if at all, as well as set time limits as to how long they can be on their computer. There are even settings that enable a parent to prevent their children from using their Mac at all during specific hours, such as during bedtime on school nights. Moreover, these settings provide parents with logs of what their children were doing while using their Macs. These controls are account based, providing a parent with two children, for example, the flexibility to apply different levels of parental controls necessary to manage activities appropriate for their 8 year old versus those appropriate for their 14 year old teenager – levels which are unlikely to be the same.

On Apple's iOS mobile devices, parents can use the Restrictions settings to prevent their children from accessing specific device features, including Location Services (discussed in detail below), as well as restricting by age level Music, Movies, TV Shows, or Apps, and also prohibiting In-App purchases. When a parent enables these controls, the parent must enter a password (this password is separate from the device password that the Parent may set for their child). Once enabled, a parent can simply tap to switch-on and off access to various features, functions and Apps, even restricting access only to age appropriate content.



EXAMPLE: Above are example screenshots from the iPhone that show restrictions settings that a mother might have set for her young teenage son on his own iPhone. As you can see in this example, this teenager is not permitted to surf the Internet or watch YouTube videos. However, he is permitted to use the iPhone camera and can participate in FaceTime chats with family and friends. His mother also has given him permission to use the iTunes store on his iPhone, but restricted downloads only to age-appropriate music & podcasts, movies, and TV shows. While this sample teenager also is able to install and delete age-appropriate Apps, his mother has prohibited him from making any In-App Purchases.

We believe these innovative easy-to-use parental controls are simple and intuitive. They provide parents with the tools they need to manage their children's activities at various stages of maturity and development based on the settings they deem appropriate.

Finally, I want to make it clear to the committee that Apple does not knowingly collect any personal information from children under 13. We state this prominently in our Privacy Policy. If we learn that we have inadvertently received the personal information of a child under 13, we take immediate steps to delete that information. Since we don't collect personal information from children under 13, we only allow iTunes store accounts for individuals 13 or over. With respect to our iAd network, our policy is that we don't serve iAds into apps for children. Further, we make it very clear in our App Store Review Guidelines that any App that targets minors for data collection will be rejected.

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

As we stated in our testimony last summer, 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.

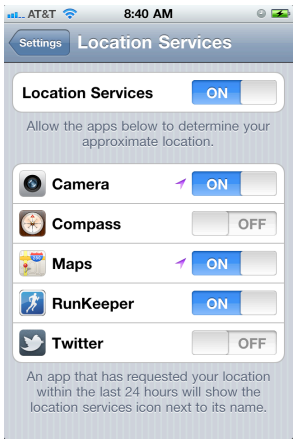
Apple offers location-based services on a variety of mobile devices, including the iPhone 3G, iPhone 3GS, iPhone 4 CDMA and GSM models, iPad Wi-Fi + 3G, iPad 2 Wi-Fi and 3G and, to a more limited extent, older models of the iPhone, the iPad Wi-Fi, and iPod touch.

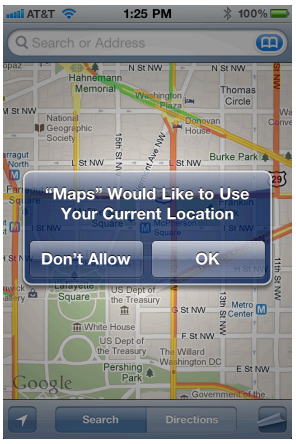
All of Apple's mobile devices run on Apple's proprietary mobile operating system, iOS. Apple released iOS 4.1 on September 8, 2010. Apple released the current versions, iOS 4.3.3 and 4.2.8 (for the iPhone 4 CDMA model), on May 4, 2011. Currently, iOS 4.3.3 may be run on

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. Location-Based Privacy Features

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





First, as you can see in the iPhone screenshots above, 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 hot spots 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 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

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

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 hotspots[5] 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 the device to calculate an initial approximate location before Apple's servers can respond to a request for information from the crowd-sourced database.

One useful way to think of our cell tower and Wi-Fi hotspot database is to compare it to a world map, like the Rand McNally World Atlas, for example. Like a world map, our database of cell towers and Wi-Fi hotspots contains the specific locations of cell towers and Wi-Fi hotspots we have gathered. It doesn't have any information about where any individual person or iPhone is located on that map at any time. The cache on your iPhone is like a series of localized city street maps. When you enter a new area that you haven't been to or haven't been for awhile, we download a subset of the World Atlas – a more localized map of cell towers and Wi-Fi hotspots to your iPhone for the iPhone itself to better assist you. Just as a street map of a city includes all the streets and intersections for many miles around you, it also has the street you are on in addition to all the streets around you, but it doesn't know where

---

[4] For 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.

[5] For 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.

[6] Cell 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.

you are at any time nor where you go or how often you go there. You use a street map to determine your precise location, relative to fixed points that are identified on the map. Similarly, your iPhone uses the fixed locations of the cell towers and WiFi hotspots to determine its own location relative to those points. Your iPhone, not Apple, determines its actual location without any further contact with Apple once it receives the city maps. Apple has no knowledge of your precise location.

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 4.3.3) Apple released on May 4, 2011, 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 re-calculate 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, 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 with Apple, pay a fee, and sign a licensing agreement before getting an app on the App Store. The current licensing agreement contains numerous provisions governing the collection and use of user data, device data, and location-based information, including the following:

- Developers and their Applications may not collect user or device data without prior user consent, and then only to provide a service or function that is directly relevant to the use of the Application, or to serve advertising;

- Applications must notify and obtain consent from each customer before location data is collected, transmitted, or otherwise used by developers;

- Developers may not use analytics software in their Applications to collect and send device data to a third party;

- Developers must provide clear and complete information to users regarding their collection, use and disclosure of user or device data (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' data from unauthorized use, disclosure or access by third parties.

- If the customer denies or withdraws consent, applications may not collect, transmit, process or utilize the customer's user or device data, including location data;

- Developers must take appropriate steps to protect customers' location-based information from unauthorized use or access;

- Developers must comply with all applicable privacy and data collection laws and regulations regarding the use or transmission of user and device data, including location-based information;

- Applications must not disable, override, or otherwise interfere with Apple-implemented system alerts, display panels, consent panels and the like, 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 our licensing agreement with any developer that 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.

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 clearly in Apple's privacy policy as well as in all relevant Apple device software licensing agreements, 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.