

Apple's Responses to Senator Al Franken's May 18, 2011 Questions

- 1. Will Apple commit to requiring that all apps in the Apple App Store have a clear, understandable privacy policy?**

Response:

For Apple's response to this question, please see the attached June 1, 2011 letter responding to Senator Franken's May 25, 2011 letter.

- 2. If not, will Apple at least commit to requiring that all location-aware apps in the Apple App Store have a clear, understandable privacy policy?**

Response:

For Apple's response to this question, please see the attached June 1, 2011 letter responding to Senator Franken's May 25, 2011 letter.

- 3. In your testimony you said that requiring apps to have privacy policies is not enough to protect user's privacy. I agree. What further steps can you take, in addition to requiring privacy policies, that will help users understand where their information is going and have greater control over it?**

Response:

Apple has taken steps to help customers understand where their information is going and to provide customers with greater control over it. First, Apple's Privacy Policy, which is available from links on every page of Apple's website, contains express disclosures regarding Apple's collection and use of location data and non-personal information:

Location-Based Services

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.

Collection and Use of Non-Personal Information

We also collect non-personal information – data in a form that does not permit direct association with any specific individual. We may collect, use, transfer, and disclose non-personal information for any purpose. The following are some examples of non-personal information that we collect and how we may use it:

- We may collect information such as occupation, language, zip code, area code, unique device identifier, location, and the time zone where an Apple product is used so that we can better understand customer behavior and improve our products, services, and advertising.

...

If we do combine non-personal information with personal information the combined information will be treated as personal information for as long as it remains combined.

Second, Apple's Software License Agreements for products that provide location-based services provide express disclosures regarding Apple's collection and use of location information. For example, to activate an iPhone, the customer must accept and agree to the iPhone SLA, including the following provision regarding location data:

4. Consent to Use of Data.

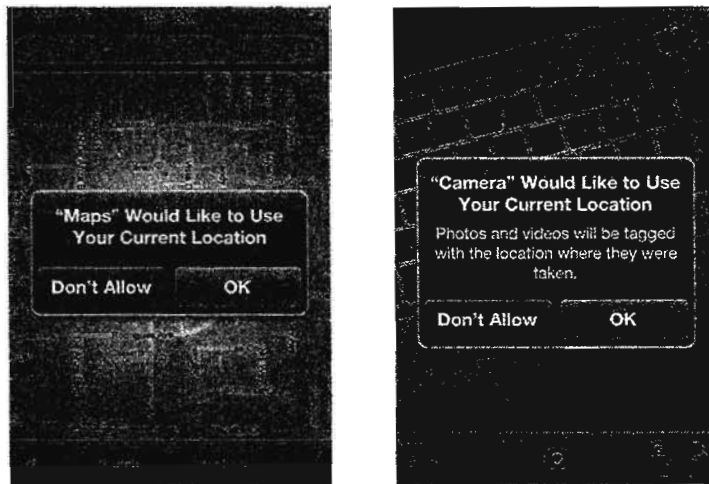
...

(b) Location Data. 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 third party's terms and privacy policy on use of location data by such third party applications or services. ...

At all times your information will be treated in accordance with Apple's Privacy Policy, which is incorporated by reference into this License and can be viewed at: www.apple.com/legal/privacy/.

Third, as described above, before any app can access or use location information, iOS, the device's operating system, discloses to the customer that the app "would like to use [the customer's] current location" and requests the customer's express consent.



Fourth, before Apple will collect any diagnostic information from an iOS customer, that customer must explicitly agree that Apple may collect and use such information. For example, iPhone customers must click "Agree" in response to the following disclosure:

You can help Apple improve its products by sending us anonymous diagnostic and usage information about your iPhone.

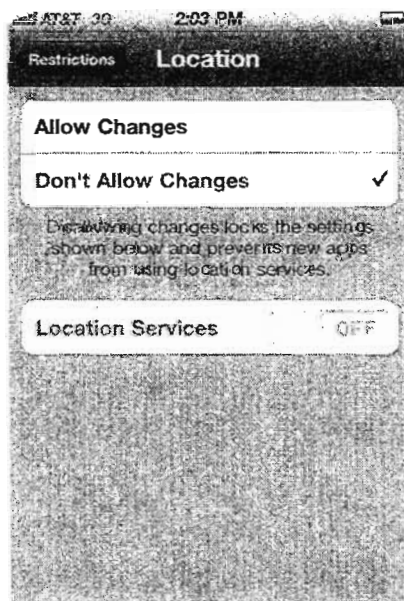
By clicking "Agree" you agree that Apple may periodically collect and use this information as part of its support services and to improve its products and services. This information is collected anonymously. To learn more about Apple's Privacy Policy, see <http://www.apple.com/legal/privacy>.

Fifth, Apple provides its customers with functionality to control the location-based service capabilities of their devices. Apple has always required express customer consent, as described above, when any app requests location-based information for the first time. If the customer does not consent, iOS will not provide any location-based information to the app. iOS also permits customers to identify individual apps that may not access location-based information, even if Location Services is on.



Customers can change their individual app settings at any time. As mentioned in Dr. Tribble's May 20, 2011 testimony, an arrow icon (↗) alerts customers that an app is using or has recently used location-based information. This icon appears in real-time for currently running apps and next to the "On/Off" toggle switch for any app that has used location-based information in the past twenty-four hours.

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. In addition, iOS will not (1)

provide any location information to any apps, including apps that may have previously received consent to use location information; (2) collect or geo-tag information about nearby Wi-Fi hotspots or cell towers; or (3) upload any location information to Apple from the device.

Finally, for iOS versions 4.1 and later, if the customer turns Location Services off, the mobile device does not send geo-tagged data about Wi-Fi hotspots and cell towers to Apple.

Apple's recent public statements and testimony have also provided customers with more information about how Apple and Apple devices use location information.

Apple is always investigating new ways to improve its customers' experiences, including helping customers learn more about Apple's privacy policy and the privacy protections available on Apple mobile devices.

4. Will Apple commit to informing users through a clear, conspicuous method (i.e. a permission screen) of the non-location information (i.e. calendar information, address book information, etc.) that an app will access once it is downloaded onto an Apple mobile device?

Response:

Apple is committed to the protection of all user personal data. As described in Apple's previous responses and testimony, Apple requires that all third-party app developers provide clear and complete information to customers regarding the collection, use and disclosure of any user or device data.

Specifically, third-party app developers must register with Apple, pay a fee, and sign a licensing agreement containing numerous provisions governing the collection and use of user data, device data, and location-based information, including the following:

- The developer must provide clear and complete information to users regarding the developer's collection, use and disclosure of user or device data (e.g., the developer must include a description on the App Store or add a link to the applicable privacy policy);
- The developer may collect, use, or disclose to a third party user or device data only with the customer's prior consent and to provide a service or function that is directly relevant to the use of the app;
- If the customer denies or withdraws consent, apps may not collect, transmit, process or utilize the customer's user or device data;
- The developer must take appropriate steps to protect customers' user and device data from unauthorized use, disclosure, or access by third parties;
- The developer must comply with all applicable privacy and data collection laws and regulations regarding the use or transmission of user and device data;

- The app 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.

Apps submitted to Apple for placement in the App Store that fail to comply with these rules are returned to the developer to be fixed. If the developer successfully corrects the app, it goes into the App Store; if not, Apple will not offer the app to its customers.

Product improvement and evolution at Apple is a way of life. We are constantly examining ways to improve the user experience and the functionality of our devices. This applies to privacy just as much as it does to every other product or service we offer. We will continue to investigate new ways to offer user enhancements in the area of data protection.

5. Will Apple 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?

Response:

Please see response to Question No.4 above.

As described in greater detail below, Apple has also documented in the App Store Review Guidelines a set of technical, content, and design criteria that every app must satisfy before Apple will accept the app for inclusion in the App Store. Pursuant to these Guidelines:

- “Apps cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used.”
- Developers and apps “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. [Developers] may not use analytics software in [their] Application to collect and send device data to a third party.”

Apps submitted to Apple for inclusion in the App Store that fail either of these requirements are returned to the developer and are not offered in the App Store until the deficiency is corrected.

6. Apple appears to acknowledge that it has not done enough to educate users about how their location information is being used. See Apple Q&A on Location Data, April 27, 2011 ("Users are confused, partly because the creators of this new technology (including Apple) have not provided enough education about these issues to date.") Can you explain how Apple will improve its education of users about the way their location information is gathered, used and shared by Apple and others?

Response:

In addition to the policies and systems described above, Apple's recent statements, including Apple's April 27, 2011 public Q&A on Location Data, press interviews, and testimony have provided customers with extensive information about how Apple and Apple devices use location information.

Apple is strongly committed to protecting our customers' privacy and will continue to explore new ways to educate customers about the collection and use of their location information.

7. You have said that Apple audits the applications in the App Store and that if Apple finds an app is violating the Registered Apple Developer Agreement, it will remove it from the store. Yet when I asked you at the hearing how many apps had been kicked out of the store for violating these terms, you said "zero". Do you believe that there is not a single app that is currently violating your Developer Agreement?

Response:

In response to Senator Franken's question, Dr. Tribble explained that Apple has not yet had to remove any app from the App Store because the app was improperly sharing a customer's location information with third parties. In fact, at the time of Dr. Tribble's May 10, 2011 testimony Apple was unaware of any app that had been (a) admitted into the App Store, (b) was subsequently determined to violate some aspect of the rules relating to the collection, retention or transmission of location data, (c) was not corrected after the developer was notified and given an opportunity to resolve the problem, and then (d) was "kicked out of the store" for violating these terms. As discussed below, Apple, however, has removed and continues to remove apps from the App Store for other types of violations.

As Dr. Tribble further explained, Before Apple will even consider accepting a third-party app for the App Store, the app developer must register with Apple, pay a fee, and sign developer and license agreements that contain numerous provisions governing, among other things, the collection and use of user data, device data, and location-based information, including those outlined above. Once the developer agrees to comply with these requirements, the developer may submit apps for review through Apple's approval process.

Apple performs a rigorous review of every app submitted based on a set of technical, content, and design criteria. The review criteria are documented in Apple's App Store Review Guidelines for iOS apps, which is made available to every app developer. A copy of the Guidelines is attached to these responses. The Guidelines include myriad requirements, including requirements about an app's functionality, content, and use of location or personal information. For example, the Guidelines state that:

4. Location

4.1 Apps that do not notify and obtain user consent before collecting, transmitting, or using location data will be rejected

...

4.4 Location data can only be used when directly relevant to the features and services provided by the app to the user or to support approved advertising uses

...

16. Objectionable content

16.1 Apps that present excessively objectionably or crude content will be rejected

16.2 Apps that are primarily designed to upset or disgust users will be rejected

...

17. Privacy

17.1 Apps cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used

17.2 Apps that require users to share personal information, such as email address and date of birth, in order to function will be rejected

17.3 Apps that target minors for data collection will be rejected

...

18. Pornography

18.1 Apps containing pornographic material, defined by Webster's Dictionary as "explicit descriptions or displays of sexual organs or activities intended to stimulate erotic rather than aesthetic or emotional feelings," will be rejected

18.2 Apps that contain user generated content that is frequently pornographic (ex "Chat Roulette" apps) will be rejected

...

On average, Apple rejects approximately 30% of the apps initially submitted for consideration. The most common reasons for rejection relate to functionality issues, such as the app crashing, exhibiting bugs, or not performing as advertised by the developer. But Apple will reject an app for violating any of the criteria set forth in the Guidelines and/or any of the provisions of the developer's agreements with Apple.

When Apple rejects an app, most developers respond by correcting the issue or issues that led to Apple's rejection so that the app may ultimately be accepted. Apple will not, however, accept any app in the App Store unless and until the developer and app are in full compliance with Apple's criteria and the developer agreements.

Similarly, Apple will remove from the App Store any app that is determined to be in violation of any of these requirements. Some of the most common reasons for removal of an app from the App Store relate to an app's violation of some other party's intellectual property rights, violation of some law, or use of objectionable content.

8. In Apple's May 6, 2011 response to my letter of April 27, 2011, Apple wrote that when "using only the crowd-sourced locations of Wi-Fi hotspots and cell towers... the device location calculated by iOS will only be an approximation." Please give the mean, median, and mode of how accurately the device's location can be calculated using only the crowd-sourced database Apple maintains on mobile devices. Please use precise figures, e.g. 50m, 100m, etc.

Response:

iOS can use the information in the crowd-sourced database to triangulate the device location when GPS is not available (such as when the device is indoors or in a basement). It is difficult to provide specific information regarding how accurate that determination will be because the accuracy can vary greatly based on factors such as whether the device is indoors or outdoors, in a rural or urban area, at a high or low altitude, etc. In general, iOS can calculate the device location using the crowd-sourced database to within 65 to 300 meters. The accuracy, however, will be worse than 300 meters – and, in some cases, significantly worse than 300 meters – in situations such as when the device is in very rural areas.

9. In various statements, Apple has stressed that the hotspots and cell towers in the crowd-sourced database downloaded to users' mobile devices "could be more than one hundred miles away." Please give the mean, median, and mode of the distance these hotspots and cell towers are from users' devices. Please use precise figures, e.g. 50m, 100m, etc.

Response:

As described previously, Apple downloads a subset of its crowd-sourced database content to a local cache on the device when the iOS has made a request for location information. Apple downloads the calculated locations of: (1) the hotspots and cell towers that the device can "see" (the "visible" hotspots and cell towers); (2) the hotspots and cell towers that are nearby; and (3) nearby cell location area codes.

To identify "nearby" hotspots and cell towers, Apple's servers search in the crowd-sourced database for hotspots and cell towers that are within up to a 2° North/South range and 4° East/West range of each visible hotspot and cell tower. Note that to ensure prompt response times, Apple limits the download to no more than 1600 hotspot locations and 100 cell tower

locations at any given time. Thus, Apple does not necessarily download all nearby hotspots and cell towers that fall within this North/South and East/West range.

Again, it is difficult to provide specific information regarding the distance that the hotspots and cell towers in the cached subset of the crowd-sourced database are from the device because the distance can vary greatly based on factors such as those identified above, the cellular carrier used by the device, etc. In some cases, the hotspots and cell towers could be within a range of more than one hundred miles; in other cases, they could be within a range of only a few hundred meters.

It is also important to note that the cached subset of the crowd-sourced database does not contain any information that indicates the distance of the hotspots and cell towers from the device's location at the time the cache was downloaded or at any other time. Thus, the database does not reveal that one particular hotspot may have been only a few hundred meters away while another was more than one hundred miles away. As described below in response to Question No. 10, the cached crowd-sourced database is just a localized map of the general vicinity of the device. As with a paper map, this map does not reveal the specific location of a device – it simply provides the device with the information needed for the device to determine, by looking at the map (among other things), its specific location.

10. In an interview with All Things Digital, Apple founder Steve Jobs stated that the hotspots and cell tower data in the crowd-sourced database downloaded to users' mobile devices "are not telling you anything about your location." See Hayley Tsukayama, "Post Tech: Jobs explains mobile policies, says Apple will testify in hearing," *Washington Post*, April 27. Is it Apple's position that the WiFi hotspot and cell tower data in the crowd-sourced database downloaded to users' mobile devices do not in any way communicate anything about a user's location?

Response:

As described in Apple's previous responses and testimony, the crowd-sourced database does not reveal personal or location information about any customer. The crowd-sourced database includes anonymous location information for Wi-Fi hotspots and cell towers that is derived in part from the geo-tagged hotspot and cell tower information sent by Apple devices.

Although a local cache of a subset of Apple's crowd-sourced database is temporarily stored on the iOS-based mobile device, it is not the data collected from that device or any other device – instead, it comprises the locations for hotspots and cell towers as calculated by Apple using crowd-sourced data obtained from Apple mobile devices. In addition, Apple's servers do not track what specific subsets of the crowd-sourced database are downloaded to and/or cached on a device. Thus, while the information that is downloaded is selected based on the device's location at the time of the download, Apple does not collect, track, or store what information is downloaded.

One useful way to think of the crowd-sourced database is to compare it to a world map. Like a world map, the crowd-sourced database of cell towers and Wi-Fi hotspots contains the calculated locations of cell towers and Wi-Fi hotspots that Apple has gathered. It does not have any information about where any individual person or iPhone is located on that map at any time. The cache that is temporarily stored on an iPhone is like a series of localized city street maps.

For example, consider a customer who is in Paris and wants to get information about his or her current location. The customer's iPhone will send a request to Apple's servers that indicates that the iPhone can "see" the Eiffel Tower. The Apple servers respond by returning the location of cell towers and hotspots in Paris – a local map of Paris. The iPhone uses the fixed locations of those nearby cell towers and Wi-Fi hotspots to determine its own location relative to those points. Apple's servers do not retain the initial request from the iPhone nor any record that a map of Paris was dispatched. The iPhone itself "knows" that it can "see" the Eiffel Tower and that it now has access to a map of Paris, but no record of the transaction is retained within Apple and no association exists between any individual or individual device and the sending out of the map of Paris.

The data stored in the local cache of Apple's crowd-sourced database does not communicate anything to Apple – and, specifically, does not communicate anything to Apple about a user's location.

11. Apple has acknowledged that the crowd-sourced database cache stored on the iPhone should not have kept up to a year's worth of data. See Apple Q&A on Location Data, April 27, 2011 ("The reason the iPhone stores so much data is a bug we uncovered..."). On what date did Apple employees discover this "bug"?

Response:

Apple discovered the bug in late April 2011 when Apple was investigating the O'Reilly researchers' claims that consolidated.db included a large amount of hotspot and cell tower data. The May 4, 2011 free iOS update fixed this bug. After this update, iOS will purge records that are older than seven days, and the cache will be deleted entirely when Location Services are turned off.

12. On what date did Apple learn that the iPhone was submitting location information to Apple servers even when location services were turned off?

Response:

In September 2010, Apple released iOS version 4.1. In certain iOS versions prior to version 4.1, a bug caused iOS to send anonymous, geo-tagged information about Wi-Fi hotspots and cell towers to Apple even if the customer had turned off Location Services. At the time of the version 4.1 update, Apple was not aware of this bug; however, as a result of updates to location services that were included in the version 4.1 update, the bug was eliminated.

Apple did not discover that this bug had existed or that the iOS version 4.1 update had fixed the bug until late April 2011 when Apple was investigating the O'Reilly researchers' claims that consolidated.db included a large amount of hotspot and cell tower data. At approximately the same time, Apple discovered that, because of a different bug, even when Location Services was off, Apple's servers would update the local cache of crowd-sourced location information for Wi-Fi hotspots and cell towers in response to an app request for location information. Although the local cache was updated, none of the downloaded crowd-sourced location information, or

any other location information, was provided to or disclosed to the app. Apple's May 4, 2011 free iOS update fixed this bug.

13. Under what circumstances does Apple 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)?

Response:

As described above and in Apple's previous responses and testimony, the geo-tagged information for Wi-Fi hotspots and cell towers obtained by Apple from Apple mobile devices does not identify any particular customer or device. Accordingly, even if Apple were considered subject to the provisions of 18 U.S.C. § 2702(c)(6), this information collected by Apple is not *customer records data*.

Apple's Responses to Senator Tom Coburn's May 18, 2011 Questions

1. **Mr. Tribble, in Mr. Soltani's testimony, he gave the committee an example whereby he seemed to imply that Apple had knowledge of his own iPhone's location within a few feet when he was sitting in the atrium of the Senate Hart Office Building using Wi-Fi. Your testimony states that Apple does not track users' locations. Can you clarify the seeming contradiction regarding the location data on Mr. Soltani's iPhone in his example?**

Response:

As described in Apple's previous responses and testimony, Apple does not track users' locations. In Mr. Soltani's example, iOS, the operating system running on his iPhone, not Apple, determined the iPhone's location. Apple did not obtain or record Mr. Soltani's location.

When Mr. Soltani ran an app that requested the current location of the device (apparently the Maps app), Apple would have downloaded a subset of the crowd-sourced database content to the local cache on his iPhone. Mr. Soltani's iPhone would then have been able to use the information in the local cache to calculate his approximate location. The iPhone would have performed this calculation without any further contact with Apple, and the iPhone would not have communicated the calculated location back to Apple.

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. Like a world map, our database of cell towers and Wi-Fi hotspots contains the calculated locations of cell towers and Wi-Fi hotspots we have gathered. It does not 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, Apple downloads a subset of the World Atlas – a more localized map of cell towers and Wi-Fi hotspots – to your iPhone to assist the iPhone in providing the location services you have requested. Your iPhone uses the fixed locations of the cell towers and Wi-Fi hotspots to determine its own location relative to those points. Your iPhone, not Apple, determines its actual location without any further contact with Apple. After the location is determined, it is not transmitted to Apple.

Mr. Soltani's example does not contradict Apple's explanation or previous testimony. The iPhone "knows" its location because iOS on the iPhone calculated the location. This location is not communicated to Apple.

2. **Apple states it does not sell users' personally identifiable information to third parties. However, Apple operates advertising services that are connected to mobile devices using its platform. Can you comment on how you operate your ad services, particularly whether you send targeted ads to mobile device users, and if so, what user information you collect in order to send targeted ads?**

Response:

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 apps. 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.

Customers may opt out of location-based advertising by toggling the device's location-based service capabilities Off. For customers who do not toggle location-based service capabilities 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.

Similarly, 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: <http://oo.apple.com>. For customers who do not opt-out of interest-based advertising, Apple uses information from the customer's iTunes account along with information obtained from Acxiom, a third party data aggregator, to send better targeted ads to our customers. For example, Apple may obtain information from iTunes about the customer's media preferences based on the categories of apps, movies, music, TV shows, and books downloaded by the customer – such as, "travel apps" or "documentary movies." The iAd server can then select ads that are relevant to and consistent with those media preferences – such as, ads relating to travel services or a newly-released documentary movie.

As stated in Apple's Privacy Policy, Apple uses this "personal information to help us develop, deliver, and improve our products, services, content, and advertising." Unless a customer provides express prior consent, as discussed below, Apple does not sell or 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 – in the ad – 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 app with more specific location information.

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

Response:

Advertising revenue currently makes up less than one percent of Apple's total revenue. Apple's sales of hardware and software products and related services account for the vast majority of Apple's revenue.

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

Response:

Apple offers its iAd services only to apps that have been approved for inclusion in the App Store. As discussed below in response to Question 2.c., Apple reviews all apps before adding them to the App Store to ensure, among other things, that the app complies with the provisions of Apple's developer agreements and app store review guidelines. If an app does not comply with all provisions, Apple will not add the app to the App Store or provide iAd services to the app.

In addition, Apple attempts to identify apps that appear to be targeted predominantly to children, and Apple does not provide iAd services to those apps.

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

Response:

Before Apple will even consider accepting a third-party app for the App Store, the app developer must register with Apple, pay a fee, and sign developer and license agreements that contain numerous provisions governing, among other things, the collection and use of user data, device data, and location-based information, including the following:

- The developer must provide clear and complete information to users regarding the developer's collection, use and disclosure of user or device data (e.g., the developer must include a description on the App Store or add a link to the applicable privacy policy);
- If the customer denies or withdraws consent, the app may not collect, transmit, process or utilize the customer's user or device data, including location data;
- The developer must take appropriate steps to protect customers' user and device data, including location-based information, from unauthorized use, disclosure, or access by third parties;

- The developer 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;
- The app 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.

Once the developer agrees to comply with these requirements, the developer may submit apps for review through Apple's approval process.

Apple performs a rigorous review of every app submitted based on a set of technical, content, and design criteria. The review criteria are documented in Apple's App Store Review Guidelines for iOS apps, which is made available to every app developer. A copy of the Guidelines is attached to these responses.

The Guidelines include myriad requirements, including requirements about an app's functionality, content, and use of location or personal information. For example, the Guidelines state that:

4. Location

4.1 Apps that do not notify and obtain user consent before collecting, transmitting, or using location data will be rejected

...

4.4 Location data can only be used when directly relevant to the features and services provided by the app to the user or to support approved advertising uses

...

16. Objectionable content

16.1 Apps that present excessively objectionably or crude content will be rejected

16.2 Apps that are primarily designed to upset or disgust users will be rejected

...

17. Privacy

17.1 Apps cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used

17.2 Apps that require users to share personal information, such as email address and date of birth, in order to function will be rejected

17.3 Apps that target minors for data collection will be rejected

...

18. Pornography

18.1 Apps containing pornographic material, defined by Webster's Dictionary as "explicit descriptions or displays of sexual organs or activities intended to stimulate erotic rather than aesthetic or emotional feelings," will be rejected

18.2 Apps that contain user generated content that is frequently pornographic (ex "Chat Roulette" apps) will be rejected

...

On average, Apple rejects, through its review process, approximately 30% of the apps initially submitted for consideration. The most common reasons for rejection relate to functionality issues, such as the app crashing, exhibiting bugs, or not performing as advertised by the developer. But Apple will reject an app for violating any of the criteria set forth in the Guidelines and/or any of the provisions of the developer's agreements with Apple.

When Apple rejects an app, most developers respond by correcting the issue or issues that led to Apple's rejection so that the app may ultimately be accepted. Apple will not, however, accept any app in the App Store unless and until the developer and app are in full compliance with Apple's criteria and the developer agreements.

Similarly, Apple will remove from the App Store any app that is determined to be in violation of any of these requirements. Some of the most common reasons for removal of an app from the App Store relate to an app's violation of some other party's intellectual property rights, violation of some law, or use of objectionable content.

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

Response:

Apple currently has a team of approximately 80 employees dedicated to performing the rigorous app review process described above. This process is not uniquely focused on the protection of consumer information but rather applies to testing for compliance with all of the rules pertaining to apps within the App Store. Once an app is accepted into the App Store, Apple requires the developer resubmit the app for approval if the developer wants to modify the app in any way. In some instances, however, apps have been changed after the review process and after they have been made available on the App Store.

Apple employees from several teams are responsible for addressing issues that arise with apps that are already in the App Store. For example, members of Apple's legal team routinely address issues raised by third parties who, once the app has gone public, complain that it violates some aspect of their intellectual property. Apple relies heavily on communications from other App Store users, competitors, and industry observers to alert Apple that an app that is operating outside of Apple's Guidelines. Whenever such a case is brought to

Apple's attention, either through internal vigilance or by an external party, Apple investigates and provides the developer with an opportunity to remediate. If no correction is made, Apple removes the app from the App Store.

- 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?**

Response:

There are numerous and robust efforts underway in industry trade associations and think tanks partnering with industry aimed at addressing the unique challenges presented by mobile devices and location based services, including issues related to privacy. Apple is aware of at least the following groups already actively working on these issues: CTIA (The Wireless Association), ACT (Association for Competitive Technology), CEA (Consumer Electronic Association), ITI (Information Technology Industry Council), TechAmerica, Center for Democracy and Technology (CDT).

Apple's Responses to Senator Richard Blumenthal's May 18, 2011 Questions

- 1. Has your company ever contemplated, implemented, or purchased information derived from the interception of wireless data transmissions traveling between third party computers and wireless access points for any purpose? If so:**

Response:

No. Apple has never intercepted wireless data transmissions between third party computers and Wi-Fi hotspots.

As described in Apple's previous responses and testimony, Apple collects anonymous location information about Wi-Fi hotspots from broadcast messages transmitted by the hotspots. Such broadcast messages are not transmissions directed between any specific third party computer and the hotspot, but are instead messages, or "beacons," broadcast by the hotspot that do not identify any intended recipient.

Also as described previously, Apple pays a fee to Skyhook Wireless ("Skyhook") for access to Skyhook's location data for Wi-Fi hotspots. Apple has no information indicating that any of the location data obtained from Skyhook was derived from the interception of wireless data transmissions between third party computers and wireless access points; however, Apple cannot speak to the specifics of Skyhook's technology.

Note that in connection with testing and debugging network performance issues with iOS, Apple's mobile device operating system, and Mac OS X, Apple's laptop and computer operating system, Apple may perform targeted diagnostic monitoring of network performance on Apple Wi-Fi networks and, occasionally, on a public Wi-Fi network based on specific feedback received about network performance on that public network. Apple does not use any diagnostic information obtained from such monitoring for location-based services; the diagnostic information is used solely for the purpose of improving product network performance.

- A. Please indicate any and all foreign and domestic jurisdictions where your company has contemplated, implemented, or purchased information derived from the interception of wireless data transmissions described above.**

Response:

N/A

- B. Please indicate any and all purpose(s) underlying any such signal interceptions.**

Response:

N/A

- C. Please provide a precise timeline of events related to the interception of wireless data transmissions by your company and/or the purchase of information derived**

from such interceptions, including when such interceptions were initially contemplated, initially implemented, and subsequently revised, if applicable.

Response:

N/A

- D. Please describe any and all methods initially contemplated and/or implemented for these purposes.

Response:

N/A

- E. Subsequent to any initial steps toward intercepting wireless data transmissions, please describe any and all methods subsequently contemplated and/or implemented for these purposes.

Response:

N/A

- F. Please indicate any and all types of data captured from signals traveling between third party computers and wireless access points that that your company has ever intercepted, stored, or purchased (including but not limited to data frames, management frames, control frames, payload data, SSIDs, RSSI measurements, etc.). For each category of data, please define the term used to reference that category, including an indication of how it is derived.

Response:

N/A

- G. Please provide text and citations for any and all materials directly or indirectly associated with your company that describe or contemplate methods for intercepting wireless data transmissions traveling between third party computers and wireless access points (including foreign or domestic patents, patent applications, published works, or other publicly available materials).

Response:

N/A

- H. Do all of the methods (described in 1.D.) contemplated or implemented by your company (or implemented by other companies from whom you subsequently purchased derived data) for intercepting wireless data transmissions explicitly exclude the interception of "content data" transmitted between third party users and wireless access points? *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

1) If so, please explain how and why such content data is excluded from interception.

2) If not, please explain how and why such content data is not excluded from interception.

Response:

N/A

- I. Do any of the methods (described in 1.D.) contemplated or implemented by your company for intercepting wireless data transmissions utilize the interception of "content data" transmitted between third party users and wireless access points to facilitate the underlying purpose of intercepting that data? If so, please explain how and why such content data is utilized. *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

Response:

N/A

- J. Has your company ever contemplated, implemented, or purchased information derived from the interception of wireless data transmissions traveling between third party computers and encrypted wireless access points and/or hidden wireless access points? If so, please explain how these methods differ from the methods associated with the interception of wireless data transmissions traveling between third parties and unencrypted wireless access points, if at all.

Response:

N/A

- K. Has your company ever shared, sold, or distributed information acquired through interception and storage of wireless data transmissions traveling between third parties and wireless access points? If so, to whom and for what purpose(s)?

Response:

N/A

- 2. Has your company ever contemplated, constructed, or purchased information related to the location of wireless access points? If so, please ensure that Questions 1.A. through 1.H. are fully answered with respect to the purpose of locating wireless access points.**

Response:

Yes, 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 in Apple's previous responses and testimony, Apple collects from millions of Apple devices anonymous location information for cell towers and Wi-Fi hotspots. 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.

Apple collects this location-based information for only one purpose – to enhance and improve the services we can offer to our customers.

As noted above, Apple does not collect or derive information about Wi-Fi hotspots from the interception of wireless data transmissions between third party computers and Wi-Fi hotspots. Instead, Apple mobile devices collect information about Wi-Fi hotspots that the devices can "see" from broadcast messages transmitted by the hotspots. The devices then tag that information with the device's current GPS coordinates, i.e., the devices "geo-tag" the hotspots.

This collected Wi-Fi hotspot and cell tower information is temporarily saved in a local cache on the device. Every twelve hours, or later if the device does not have Wi-Fi access at that time, that data is extracted from the database, encrypted, and transmitted – anonymously – to Apple over a Wi-Fi connection. (Note that as of Apple's May 4, 2011 free iOS software update, iOS will clear this data from the local cache after twenty-four hours, even if the device never had Wi-Fi access and, thus, was not able to transmit the data to Apple.) 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 app's request to use location information.

In addition, for computers and laptops running Apple's Mac OS X operating system and mobile devices running older versions of Apple's mobile operating system (iPhone OS versions 1.1.3 to 3.1), Apple relied on (and still relies on) a database of Wi-Fi hotspot location information maintained by Skyhook. Beginning with iOS version 3.2 released in April 2010, Apple relies on its own crowd-sourced database of Wi-Fi hotspot location information.

As noted above, Apple has no information indicating that any of the data that Apple obtained from Skyhook was derived from the interception of wireless data transmissions between third party computers and wireless access points. Apple cannot, however, speak to the specifics of Skyhook's technology.

A. How many wireless access points exist, or have ever existed, in any database of wireless access point locations?

Response:

As of March 22, 2011, Apple's crowd-sourced database includes approximately 223 million active Wi-Fi hotspots.

1) How many of these wireless access points were unencrypted when identified?

Response:

Apple does not collect information about the encryption scheme of Wi-Fi hotspots and, thus, does not know how many of these hotspots were unencrypted.

2) How many of these wireless access points were encrypted when identified?

Response:

Apple does not collect information about the encryption scheme of Wi-Fi hotspots and, thus, does not know how many of these hotspots were encrypted.

3) How many of these wireless access points were "hidden" when identified?

Response:

On March 2, 2011, with the release of iOS version 4.3, iOS first began collecting from hotspot broadcasts a single Boolean value indicating whether the SSID is or is not present for the hotspot (i.e., whether the hotspot is or is not "hidden"). Note that Apple does not collect the SSID for any hotspot, regardless of whether or not the hotspot is hidden. Because Apple only recently started collecting the Boolean value indicating whether the hotspot is or is not hidden, Apple does not yet have statistical information available for how many hotspots were "hidden."

3. Please describe any and all ways in which the interception and/or storage of “content data” transmitted between third party users and wireless access points might be:

A. Indirectly valuable for effectuating the purpose of efficiently locating wireless access points; and

Response:

Apple does not intercept or store “content data” transmitted between third party users and wireless access points for locating wireless access points.

Apple is aware of public studies, papers, and patents discussing the use of content or payload data, payload transmissions, and bit-error rates for certain location purposes. Apple does not implement any of these techniques.

B. Indirectly valuable to your company for any other purpose.

Response:

Again, Apple does not intercept or store “content data” transmitted between third party users and wireless access points and does not have an opinion regarding how such information might or might not be valuable for any other purpose.

4. Please describe your view of the circumstances under which the interception and/or storage of “content data” transmitted between third party users and wireless access points might be:

A. Legal or illegal under current federal law;

Response:

Apple does not intercept or store “content data” transmitted between third party users and wireless access points and, thus, does not have an opinion regarding whether such interception and/or storage is or is not legal under current federal law.

B. Legal or illegal under current state law; and

Response:

Apple does not intercept or store “content data” transmitted between third party users and wireless access points and, thus, does not have an opinion regarding whether such interception and/or storage is or is not legal under the current laws of any state.

- C. Legal or illegal in any foreign jurisdictions in which your company has engaged in the interception and/or storage of wireless data transmissions traveling between third party computers and wireless access points.**

Response:

Apple does not intercept or store "content data" transmitted between third party users and wireless access points and, thus, does not have an opinion regarding whether such interception and/or storage is or is not legal under the laws of any foreign country.