FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED TWELFTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115

Majority (202) 225–2927
Minority (202) 225–3641

April 25, 2011

Mr. Steve Jobs
C.E.O.
Apple Inc.
One Infinite Loop
Cupertino, CA 95014

Dear Mr. Jobs:

We write to you to request information regarding an important privacy issue. Recent press reports suggest that mobile wireless devices running Apple's iOS version 4.0 and later versions compile a history of the locations visited by their users and automatically store this data both on the devices and in the backups created by synching the devices with iTunes. So that we may better understand the nature of the location data that smartphones running your operating system track, use, store, and share, and evaluate any related privacy issues, please answer the following questions:

1. What location data do devices running your operating system track, use, store, or share?

2. Why does the device track, use, store, or share that data?

3. Where on the device is the data stored; how is it used, stored, or shared; and how is it protected?

4. How is that data accessible and who can access it? Is the data automatically transferred to your company or to other devices, or to third parties? If so, how and why? Is there any other manner in which the data can be transferred to or obtained by your company, or by other devices, or by third parties and, if so, how and why?

5. Is the user informed of, or given an opportunity to prevent, such tracking, use, storing, or sharing of data and, if so, how? Can the end-user disable the tracking, use, storing, and sharing of such data? Can the user delete the data?

6. How long does the device store the data?

7. Section 222 of the Communications Act contains privacy provisions. Do those provisions apply to you? Should they? Does it make sense that similar information is afforded different privacy protections depending on what entity does the collecting and what service the data is collected from, especially since the entities collecting such information are increasingly competing against each other in today's information age?

8. In a July 12, 2010, response to a June 24, 2010, letter from Reps. Joe Barton and Edward Markey, both of which we attach to this letter, you outlined some of your location data collection practices and privacy policies. Are your current location data collection practices the same as the practices you described in your July 12, 2010, letter? If not, how have those practices changed, and have you notified consumers and Congress of those changes?

9. Are you currently planning to implement any measures to address the privacy concerns referenced above?

Please provide responses to these questions no later than May 9, 2011. If you have any questions, please contact a member of our Committee staff at (202) 225-2927.

Sincerely,

Fred Upton
Chairman

Greg Walden
Chairman
Subcommittee on Communications
and Technology

Mary Bono Mack
Chairman
Subcommittee on Commerce, Manufacturing
and Trade

Lee Terry
Vice Chairman
Subcommittee on Communications
and Technology

Marsha Blackburn
Vice Chairman
Subcommittee on Commerce, Manufacturing,
and Trade

Attachments

cc: The Honorable Henry A. Waxman, Ranking Member

The Honorable Anna G. Eshoo, Ranking Member
Subcommittee on Communications and Technology

The Honorable G. K. Butterfield, Ranking Member
Subcommittee on Commerce, Manufacturing, and Trade

Congress of the United States
Washington, DC 20515

June 24, 2010

Mr. Steve Jobs
Chief Executive Officer
Apple Inc.
1 Infinite Loop
Cupertino, CA 95014

Dear Mr. Jobs:

We are writing in response to press reports ("Apple Collecting, Sharing iPhone Users Precise Locations," Los Angeles Times, June 21, 2010) highlighting recent changes in Apple's privacy policy. The updated terms and conditions suggest that Apple is collecting and sharing data containing the precise geographic locations of consumers using iPads, iPhones, and other Apple products.

It is our understanding that Apple's consumers cannot use newly-purchased iPads, iPhones, Apple computers, or purchase products for existing Apple products from the iTunes music store unless they accept the revised terms and conditions and include agreeing to the collection and sharing of geographical location data. Given the limited ability of Apple users to opt out of the revised policy and still be able to take advantage of the features of their Apple products, we are concerned about the impact the collection of such data could have on the privacy of Apple's customers. To better understand the nature of Apple's data collection practices, its possible impact on consumers, and the broader public policy implications of the data usage, we request responses to the following questions.

1. Which specific Apple products are being used by Apple to collect geographic location data?
2. When did Apple begin collecting this location data, and how often is data collected from a given consumer?
3. Does Apple collect this location data from all consumers using Apple products? If the answer is no, please explain which consumers Apple is collecting information from and the reasons that these consumers were chosen for monitoring.
4. How many consumers are subject to this collection of location data?
5. What internal procedures are in place to ensure that any location data is stored "anonymously in a form that does not personally identify" individual consumers?
6. Please explain in detail why Apple decided to begin collecting location data at this time, and how it intends to use the data.
7. Is Apple sharing consumer location information collected through iPhones and iPads with AT&T or other telecommunications carriers?

PRINTED ON RECYCLED PAPER

8. Who are the unspecified "partners and licensees" with which Apple shares this location data, and what are the terms and conditions of such information sharing? How does this comply with the requirements of Section 222 of the Communications Act, which mandates that no consumer location information be shared without the explicit prior consent of the consumer?
9. Does Apple believe that legal boilerplate in a general information policy, which the consumer must agree to in order to download applications or updates, is fully consistent with the intent of Section 222, and sufficient to inform the consumer that the consumer's location may be disclosed to other parties? Has Apple or its legal counsel conducted an analysis of this issue? If yes, please provide a copy. If not, why not?

Thank you in advance for your attention to this matter. We respectfully request a response by July 12, 2010.

Sincerely,

Edward Markey

Joe Barton

July 12, 2010

VIA HAND DELIVERY

The Honorable Edward J. Markey
The Honorable Joe Barton
United States House of Representatives
Washington, DC 20515

Re: ***Apple Inc.'s Response to Request for Information Regarding Its Privacy Policy and Location-Based Services***

Dear Representatives Markey and Barton:

I write in response to your June 24, 2010 letter to Steve Jobs requesting information and documents about Apple's privacy policy and location-based services. I appreciate the opportunity to provide additional information about these matters, and I welcome further discussions with you.

To provide context to our responses to the questions presented in your letter, I first would like to provide some background information about Apple's privacy policy, location-based services, the iAd network, and the App Store.

I. APPLE'S PRIVACY POLICY

A. Overview

Apple is strongly committed to protecting the privacy of its customers. Apple has a single Customer Privacy Policy (the "Policy") that applies across all Apple businesses and products, including the iTunes Store and App Store.[1] 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.[2]

As noted in your letter, the Policy was updated on June 21, 2010, to add, among other changes discussed below, the following provision regarding location-based information:

---

[1] As used in the policy and in this letter, "Apple," refers to Apple Inc. and affiliated companies.
[2] The links take customers to http://www.apple.com/legal/privacy, which may also be accessed by customers directly.

> 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 incorporated 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 3GS SLA, last updated in May 2009, states:

> Apple and its partners and licensees may provide certain services through your iPhone that rely upon location information. To provide 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 collected by Apple is collected in a form that does not personally identify you and may be used by Apple and its partners and licensees to provide 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 to provide such products and services.** You may withdraw this consent at any time by not using the location-based features or by turning off the Location Services setting 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.

(Emphasis in original.) Similar provisions regarding location-based information appear in the iPhone 4, iPad, iPod Touch, Mac OS X, and Safari 5 SLAs.

The Policy identifies dedicated email addresses for privacy-related inquiries and comments. Apple monitors these email addresses 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.

B. June 2010 Policy Update

In the past three years, Apple revised its Policy three times: June 29, 2007, early February 2008, and June 21, 2010.

The June 29, 2007 update advised customers about the necessary exchange of information between Apple and the relevant cellular carrier when an iPhone is activated. Apple also added a provision stating that it does "not knowingly collect personal information from children." The provision explained that if such information was collected inadvertently, Apple would attempt to delete it "as soon as possible."

The February 2008 Policy update revised language regarding Apple's use of "pixel tags." Pixel tags are tiny graphic images used to determine what parts of Apple's website customers visited or to measure the effectiveness of searches performed on Apple's website. The revised language stated that: "[Apple] may use this information to reduce or eliminate messages sent to a customer."

On June 21, 2010, Apple updated the Policy to incorporate the language regarding location-based services from Apple SLAs, as discussed above. Apple also added provisions regarding new Apple services, such as Apple's MobileMe "Find My iPhone" feature and the iAd network. Apple made the following, additional material changes to the Policy:

- Revised provisions regarding (i) what information Apple collects from customers and how Apple and its partners and licensees may use the information, (ii) the use of "Cookies and Other Technologies," (iii) the safeguards in place to prevent the collection of personal information from children, and (iv) the collection and use of information from international customers; and

- Added provisions (i) advising customers to review the privacy practices of third-party application providers and (ii) cautioning customers about posting personal information on an Apple forum, chat room, or social networking service.

As noted above, customers may access the updated Policy from every page on Apple's website. The updated Policy also was placed where Apple believed the largest number of customers would see it: the iTunes Store. Following the update, every customer logging onto the iTunes Store is prompted to review the iTunes Store Terms and Conditions. For customers with existing iTunes accounts, the webpage states:

> iTunes Store Terms and Conditions have changed. Apple's Privacy Policy
>
> The changes we have made to the terms and conditions include the following:

• Apple's Privacy Policy has changed in material ways. Please visit www.apple.com/legal/privacy or view below.

Customers are 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 will not be able to use the iTunes Store (*e.g.*, will not be able to make purchases on the iTunes Store or the App Store), but they may continue to use iTunes software.

Customers attempting to open a new iTunes 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." Customers who do not accept the Terms and Conditions and the Policy will not be able to open an iTunes account but may still activate and use their devices.

II. LOCATION-BASED SERVICES

A. Overview

In response to increasing customer demand, Apple began to provide 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, locating their friends or letting their friends know where they are, or identifying nearby restaurants or stores.

Apple offers location-based services on the iPhone 3G, iPhone 3GS, iPhone 4, iPad Wi-Fi + 3G, and, to a more limited extent, older models of the iPhone, the iPad Wi-Fi, iPod touch, Mac computers running Snow Leopard,[3] and Windows or Mac computers running Safari 5.[4]

Although Apple's customers value these services and may use them on a daily basis, Apple recognizes that some customers may not be interested in such services at all times. As discussed below, Apple provides its customers with tools to control if and when location-based information is collected from them.

B. Privacy Features

Apple has always provided its customers with the ability to control the location-based service capabilities of their devices. In fact, Apple now provides customers even greater control

---

[3] All of Apple's Mac computers, *e.g.*, MacBook, MacBook Pro, MacBook Air, iMac, Mac mini, and Mac Pro, run on its proprietary Mac OS operating system. Apple released the current version, Mac OS X version 10.6, known as "Snow Leopard," on August 28, 2009.

[4] Safari is Apple's proprietary Internet browser. Apple released the current version of Safari version 5, on June 7, 2010.

over such capabilities for devices running the current version of Apple's mobile operating system—iOS 4.[5]

First, customers have always had 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 "General" menu under "Settings." For Mac computers running Snow Leopard, the toggle switch is in the "Security" menu under "System Preferences." And for Safari 5, the toggle switch is in the "Security" menu in Safari "Preferences." If customers toggle the switch to "Off," they may not use location-based services, and no location-based information will be collected.

Second, Apple has always required express customer consent when any application or website requests location-based information for the first time. When an application or website requests the information, a dialogue box appears stating: "[Application/Website] would like to use your current location." The customer is asked: "Don't Allow" or "OK." If the customer clicks on "Don't Allow," no location-based information will be collected or transmitted. This dialogue box is mandatory—neither Apple nor 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 though the global location-based service capabilities setting may be toggled to "On." The "General" menu under "Settings" provides an "On/Off" toggle switch for each application. When the switch for a particular application is toggled to "Off," no location-based information will be collected or transmitted for that application. And even if the switch for an application is toggled to "On," the "Don't Allow/OK" dialogue box will request confirmation from the customer the first time that application requests location-based information. Customers can change their individual application settings at any time.

Finally, 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" toggle switch for any application that has used location-based information in the past twenty-four hours.

C. Location-Based Information

To provide the high quality products and services that its customers demand, Apple must have access to comprehensive location-based information. 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-

[5] All of Apple's mobile devices run on its proprietary mobile operating system. Apple released the current version, iOS 4, on June 21, 2010. Currently, iOS 4 may be run on the iPhone 3G, iPhone 3GS, iPhone 4, and iPod touch. The iPad Wi-Fi + 3G, iPad Wi-Fi, and older models of the iPhone run on prior versions of Apple's mobile operating system, referred to as iPhone OS. Apple has released iPhone OS versions 1.0 through 3.2.

based services and for diagnostic purposes. These databases 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. Apple always has taken great care to protect the privacy of its customers.

1. Cell Tower and Wi-Fi Information

a. Collections and Transmissions from Apple Mobile Devices

To provide location-based services, Apple must be able to determine quickly and precisely where a device is located. To do this, Apple maintains a secure database containing information regarding known locations of cell towers and Wi-Fi access points. The information is stored in a database accessible only by Apple and does not reveal personal information about any customer.

Information about nearby cell towers and Wi-Fi access points is collected and sent to Apple with the GPS coordinates of the device, if available: (1) when a customer requests current location information and (2) automatically, in some cases, to update and maintain databases with known location information. In both cases, the device collects the following anonymous 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 unique number assigned by a manufacturer to a network adapter or network interface card ("NIC"). The address provides the means by which a computer or mobile device is able to connect to the Internet. 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").

First, when a customer requests current location information, the device encrypts and transmits Cell Tower and Wi-Fi Access Point Information and the device's GPS coordinates (if available) over a secure Wi-Fi Internet connection to Apple.[6] For requests transmitted from devices running the iPhone OS version 3.2 or iOS 4, Apple will retrieve known locations for nearby cell towers and Wi-Fi access points from its proprietary database and transmit the information back to the device. For requests transmitted from devices running prior versions of the iPhone OS, Apple transmits—anonymously—the Cell Tower Information to Google[7] and Wi-Fi Access Point Information to Skyhook. These providers return to Apple known locations of nearby cell towers and Wi-Fi access points, which Apple transmits back to the device. The device uses the information, along with GPS coordinates (if available), to determine its actual location. Information about the device's actual location is not transmitted to Apple, Skyhook, or Google. Nor is it transmitted to any third-party application provider, unless the customer expressly consents.

Second, to help Apple update and maintain its database with known location information, Apple may also collect and transmit Cell Tower and Wi-Fi Access Point Information automatically. With one exception,[8] Apple automatically collects this information only (1) if the device's location-based service capabilities are toggled to "On" and (2) the customer uses an application requiring location-based information. If both conditions are met, the device intermittently and anonymously collects Cell Tower and Wi-Fi Access Point Information from the cell towers and Wi-Fi access points that it can "see," along with the device's GPS coordinates, if available. This information is batched and then encrypted and transmitted to Apple over a Wi-Fi Internet connection every twelve hours (or later if the device does not have Wi-Fi Internet access at that time).

b. Collections and Transmissions from Computers Running Snow Leopard and/or Safari 5

Apple collects Wi-Fi Access Point Information when a Mac computer running Snow Leopard makes a location-based request—for example, if a customer asks for the current time

---

[6] Requests sent from devices running older versions of the iPhone OS also include a random identification number that is generated by the device every ninety days. This number cannot be used to identify any particular user or device.

[7] For GPS-enabled devices running prior versions of the iPhone OS, Apple also sends the device's GPS coordinates, if available, anonymously to Google so that Google can update its database of known locations.

[8] For GPS-enabled devices with location-based service capabilities toggled to "On," Apple automatically collects Wi-Fi Access Point Information and GPS coordinates when a device is searching for a cellular network, such as when the device is first turned on or trying to re-establish a dropped connection. The device searches for nearby Wi-Fi access points for approximately thirty seconds. The device collects anonymous Wi-Fi Access Point Information for those that it can "see." This information and the GPS coordinates are stored (or "batched") on the device and added to the information sent to Apple. None of the information transmitted to Apple is associated with a particular user or device.

zone to be set automatically. The information is collected anonymously and is stored in a database accessible only by Apple. Snow Leopard users can prevent the collection of this information by toggling the "Location Services" setting to "Off" in the "Security" menu under "System Preferences."

Apple also provides location-based services in Safari 5. When a customer is using Safari 5 and runs an Internet application that requests location-based information (*e.g.*, Google Maps), a dialog box will appears stating: "[Website name] would like to use your computer location." If the customer selects "Don't Allow," no location-based information is transmitted by the computer. If the customer selects "OK," Wi-Fi Access Point Information is transmitted to Apple with the request, so that Apple can return information about the computer's location. Apple does not store any Wi-Fi Access Point Information sent with requests from Safari 5.

2. Diagnostic Information

To evaluate and improve the performance of its mobile hardware and operating system, Apple collects diagnostic information from randomly-selected iPhones and analyzes the collected information. For example, when an iPhone customer makes a call, Apple may determine the device's approximate location at the beginning and end of the call to analyze whether a problem like dropped calls is occurring on the same device repeatedly or by multiple devices in the same area. Apple determines the approximate location by collecting information about nearby cell towers and Wi-Fi access points and comparing that with known cell tower and Wi-Fi access point locations in Apple's database. Apple may also collect signal strength information to identify locations with reception issues.

Before any diagnostic information is collected, the customer must provide express consent to Apple. If the customer consents, the information is sent to Apple over a secure connection. The information is sent anonymously and cannot be associated with a particular user or device. The diagnostic information is stored in a database accessible only by Apple. If the customer does not consent, Apple will not collect any diagnostic information.

3. GPS Information

The iPhone 3G, iPhone 3GS, iPhone 4, and iPad Wi-Fi + 3G are equipped with GPS chips. A GPS chip attempts to determine a device's location by analyzing how long it takes for satellite signals to reach the device. Through this analysis, the GPS chip can identify the device's latitude/longitude coordinates, altitude, speed and direction of travel, and the current date and time where the device is located ("GPS Information").

Apple collects GPS Information from mobile devices running the iPhone OS 3.2 or iOS 4. GPS Information may be used, for example, to analyze traffic patterns and density in various areas. With one exception,[9] Apple collects GPS Information only if (1) the location-based

[9] GPS Information is also collected during the short period of time (approximately thirty seconds) when a GPS-enabled device with location-based service capabilities toggled to "On" is

service capabilities of the device are toggled to "On" and (2) the customer uses an application requiring GPS capabilities. The collected GPS Information is batched on the device, encrypted, and transmitted to Apple over a secure Wi-Fi Internet connection (if available) every twelve hours with a random identification number that is generated by the device every twenty-four hours. The GPS Information cannot be associated with a particular customer or device.

The collected GPS Information is stored in a database accessible only by Apple.

D. iAd Network

On July 1, 2010, Apple launched the iAd mobile advertising network for iPhone and iPod touch devices running iOS 4. The iAd 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 updated Policy and the iPhone 4 and iPod touch 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."[10]

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.

---

searching for a cellular network. This information is sent anonymously to Apple to assist the device with locating an available channel. Apple does not retain this GPS Information in its database.

[10] A customer who opts out of interest-based and location-based advertising may still receive ads. The ads, however, will likely be less relevant to the customer because they will not be based on either interests or location. The customer also may receive interest-based or location-based ads from networks other than the iAd network.

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 dialogue box will appear stating: "iAd 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.

III. THIRD-PARTY APPLICATIONS

A. Overview

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 200,000 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.

B. Third-Party Developers

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 (PLA § 3.3.9);

- 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) (PLA § 3.3.10);

- Developers must take appropriate steps to protect customers' location-based information from unauthorized use or access (*id.*);

- Developers must comply with applicable privacy and data collection laws and regulations regarding the use or transmission of location-based information (PLA § 3.3.11);

- Applications must notify and obtain consent from each customer before location data is collected, transmitted, or otherwise used by developers (PLA § 3.3.12); 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 (PLA § 3.3.14).

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. (PLA § 12.2.)

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.

IV. RESPONSES

The following responses represent the current state of our knowledge based on our investigation to date. Our investigation is ongoing, however, and we may continue to discover information responsive to your letter. I will update our responses, as needed, if we locate other responsive materials or information.

1. **Which specific Apple products are being used by Apple to collect geographic location data?**

The iPhone 3G, iPhone 3GS, iPhone 4, iPad Wi-Fi + 3G, and, to a more limited extent, older models of the iPhone, the iPad Wi-Fi, iPod touch, Mac computers running Snow Leopard, and Windows or Mac computers running Safari 5.

2. **When did Apple begin collecting this location data, and how often is data collected from a given consumer?**

Apple first began offering location-based service in January of 2008 and began collecting Wi-Fi Access Point Information at that time.

As described above, collection of location data varies greatly based on the services requested by each customer. Location data will not be collected at all from those users who have location services turned off.

3. **Does Apple collect this location data from all consumers using Apple products? If the answer is no, please explain which consumers Apple is**

collecting information from and the reasons that these consumers were chosen for monitoring?

Apple collects anonymous Wi-Fi Access Point, Cell Tower and GPS Information from devices that have location services turned on, have explicitly authorized apps to use their location, and are actively running one of the apps. Anonymous Wi-Fi Access Point Information and GPS coordinates may also be collected when an iPhone is using GPS to search for a cellular network. Diagnostic location data is only collected from users who have expressly agreed to send this information to Apple. Device location data (by zip code only) is collected from users who participate in the iAd network.

4. **How many consumers are subject to this collection of location data?**

Please see our answer to question #3 above.

5. **What internal procedures are in place to ensure that any location data is stored "anonymously in a form that does not personally identify" individual consumers?**

When a customer's device sends Wi-Fi, cell tower, GPS or diagnostic location data to Apple it does not include any information identifying the particular device or user.

In the case of the iAd network, latitude and longitude coordinates are collected and immediately converted to a five-digit zip code. Latitude and longitude coordinates are not kept or otherwise associated with an individual. Apple's iAd server does associate the five-digit zip code with a device identifier for the purpose of serving a location-relevant ad. Apple does not share any location data 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 duplicative ads and for administrative purposes. Apple intends to retain the zip code information it has collected for six months to administer and improve the iAd network. After six months, the information may be aggregated for administrative purposes.

6. **Please explain in detail why Apple decided to begin collecting location data at this time, and how it intends to use the data.**

Please see our answer to question #2 above regarding when we began collecting relevant information. Apple collects location data for only one purpose—to enhance and improve the services we can offer to our customers.

7. **Is Apple sharing consumer location information collected through iPhones and iPads with AT&T or other telecommunications carriers?**

No.

8. **Who are the unspecified "partners and licensees" with which Apple shares this location data, and what are the terms and conditions of such information sharing? How does this comply with the requirements of Section 222 of the Communications Act, which mandates that no consumer location information be shared without the explicit prior consent of the consumer?**

The "licensees" referred to above are our software application developers. Apple shares location data with an application developer only after a user has given express consent to the sharing.

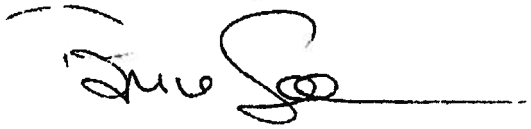
"Partners" refers to two external partners who maintain databases of known locations for cell towers and Wi-Fi access points. Earlier versions of the iPhone software rely on these databases for Wi-Fi access point and cell tower locations. For devices running that earlier software, Apple shares anonymous, non-device identifying location information with these external partners to obtain better location results for our users.

9. **Does Apple believe that legal boilerplate in a general information policy, which the consumer must agree to in order to download applications or updates, is consistent with the intent of Section 222, and sufficient to inform the consumer that the consumer's location may be disclosed to other parties? Has Apple or its legal counsel conducted an analysis of this issue? If yes, please provide a copy. If not, why not?**

While Apple is not a telecommunications carrier or service provider subject to Section 222, we believe the privacy protections described in detail in this letter are consistent with the intent of Section 222.

Apple is committed to giving our customers clear notice and control over their information, and we believe our products do this in a simple and elegant way. We share your concerns about the collection and misuse of location data, and appreciate this opportunity to explain our policies and procedures.

Sincerely,



Bruce Sewell
General Counsel and Senior Vice President of
Legal and Government Affairs