Peter B. Davidson
Senior Vice President
Federal Government Relations

1300 I Street, NW, Suite 400 West
Washington, DC 20005

Phone: 202-515-2512
peter.b.davidson@verizon.com

April 19, 2011

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

Dear Representatives Markey and Barton:

I am writing in response to your March 29, 2011 letter to Daniel S. Mead, President and Chief Executive Officer of Verizon Wireless. Verizon Wireless appreciates this opportunity to describe our practices with respect to the matters raised in your letter and to discuss our general policies and views regarding the protection of our consumers' location and other personal information.

Protecting our customers' privacy is one of Verizon Wireless' highest priorities. For years we have fought against publishing our customers' numbers in cellphone directories; we have filed more than 20 federal lawsuits against spammers, telemarketers, pretexters, and others who have sought to invade our customers' privacy; and we have adopted robust customer privacy protections to keep pace with rapidly changing technological advances. We provide customers with clear disclosures about the kinds of information we collect and use, as well as effective tools allowing them to control how their information is used. We have adopted and communicated to our customers responsible policies aimed at protecting information about them, including information obtained through location-based applications and service offerings ("location information").

Consistent with our commitment to an open network in which customers can access and download the applications of their choice, Verizon Wireless customers have access to a wide array of our own and third-party location-based applications and services. These location-based applications and services offer convenient features and tools that consumers demand, allowing them more easily to navigate roads, obtain directions, instantaneously look up weather conditions, or locate friends and family, all while on the go.

Verizon Wireless recognizes that with these new technologies come significant responsibilities to protect the information our customers entrust to us. Specifically, Verizon Wireless believes that location-based applications and services (whether provided by us or third parties such as Google) should give customers clear and transparent notice about the information that is collected and used, and empower customers to control when and how information about their individual locations can be collected, used, or shared.

To this end, as described in more detail below, Verizon Wireless takes a number of steps to inform and empower consumers with respect to the collection and use of location information. At the device level, Verizon Wireless requires manufacturers to ship devices with the general location settings turned off with respect to Verizon Wireless location-based services. (The only exception, as mandated by the FCC's E-911 regulations, is that devices are programmed to provide location information when calls to 911 are made.) This practice helps to limit the ability of Verizon Wireless and third-party applications and services to access, collect, and use location information without the customer taking affirmative steps to enable such applications and services. (This specific consent mechanism is further illustrated in the screen shot reproduced at page 5 of this letter.)

As to applications and services that access location information, some are provided by Verizon Wireless, while others are provided by third parties, such as device manufacturers, application developers, and device operating system developers. When these applications and service are provided by Verizon Wireless, Verizon Wireless only collects and uses customer location information for non-service and operational purposes, such as delivery of a locally relevant ad or coupon, upon providing clear disclosure and after obtaining the customer's affirmative consent. Verizon Wireless authorizes third-party application developers and service providers to utilize Verizon Wireless-provided technologies to obtain customer location information only if they adhere to the same disclosure and consent requirements. As to applications and services provided by third parties (without use of Verizon Wireless technologies), however, Verizon Wireless does not and indeed cannot control the collection and use of location information. Verizon Wireless therefore provides its customers with prominent notices about privacy concerns that may arise in third-party-provided location services, and gives customers tools to limit or restrict the collection and use of this information. (These specific consent mechanisms are further illustrated on pages 7-9 of this letter.)

Responses To Specific Questions

1. ***Please describe the policies and procedures your company utilizes to comply with Section 222 of the Communications Act (47 U.S.C. 222), which requires express prior authorization of the customer for use, disclosure of or access to the customer's location information for commercial purposes.***

Verizon Wireless collects and uses location information for various service and operational purposes. These include ensuring that customers have a wireless signal to complete a call and access data, transferring a wireless call or data session across a highly diverse and complex network as a mobile user moves in and out of a geographic area covered by a particular radio antenna, and maximizing network capacity and efficiency to reduce operational costs, limit "dropped" calls and ineffective data transmissions, and to provide our customers with the highest quality wireless services. As we disclose in our privacy policy, we may disclose certain information about a customer (including his or her location) in response to a court order or other legal process, such as to assist law enforcement in emergencies or in response to 911 emergency calls. Verizon Wireless has designed its commercial location-based service offerings to comply with Section 222 of the Communications Act by obtaining express prior authorization from customers before location information is used for purposes other than service delivery and operations. This is true even in situations where the location information may not qualify as Customer Proprietary Network Information ("CPNI").

For instance, Verizon Wireless' VZ Navigator application utilizes location information, allowing customers to search points of interest, pull up maps, and retrieve real-time turn-by-turn driving directions and navigation related services. Verizon Wireless requires, before any location information may be collected, used, or shared by the application, that customers turn their device location settings to the "on" position. In addition, customers must affirmatively consent to the use of their location information when opening and using the application for the first time. (This specific consent mechanism is further illustrated in the screen shots reproduced at page 10 of this letter).

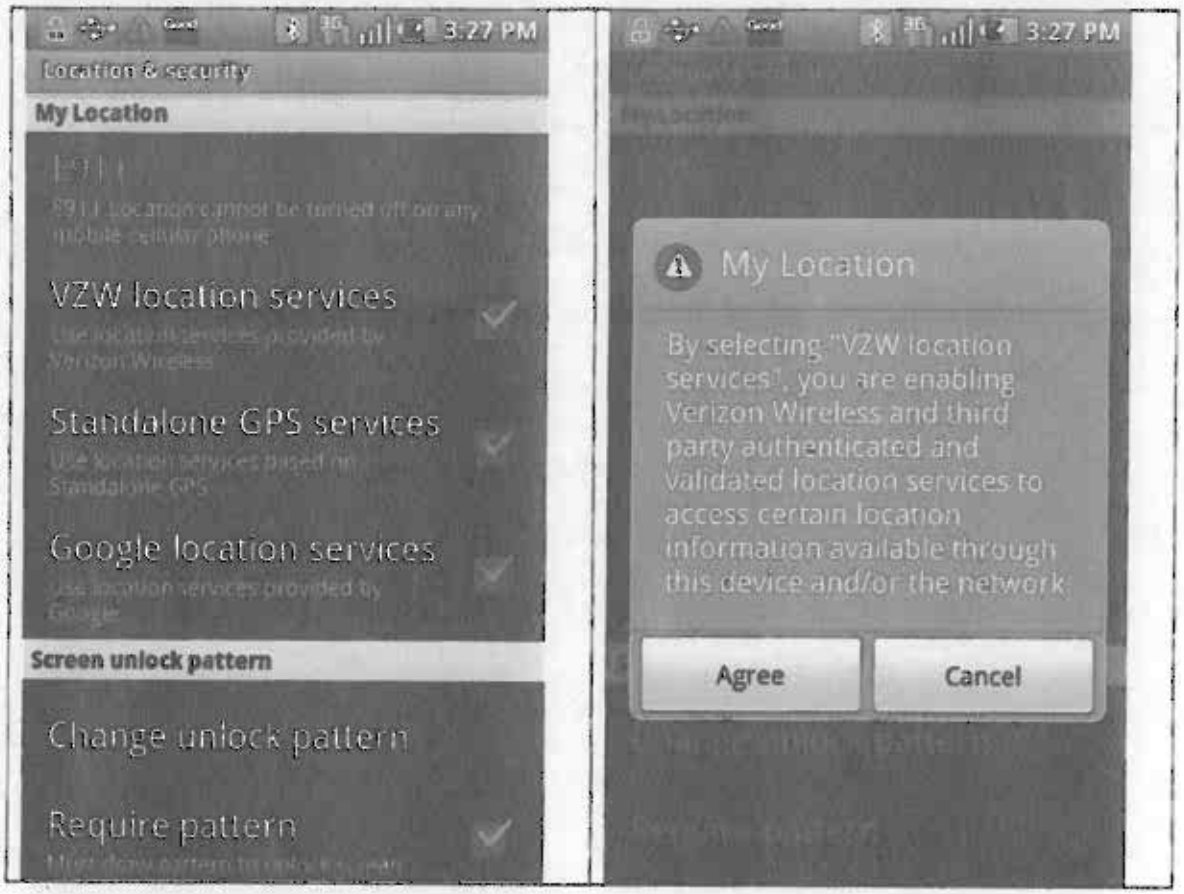
Another example is Verizon Wireless' Family Locator application, which enables customers to stay in communication with family members using maps, alerts, messages, and features like 'geo-fencing'. Verizon Wireless requires affirmative consent for all "connected" devices (which are required to be on the same account for privacy and security reasons). Similarly, with the NFL Mobile application, Verizon Wireless must identify whether a customer is within a "black-out" zone for purposes of complying with league-mandated restrictions regarding the streaming of live NFL games through the application. Verizon Wireless collects affirmative consent from customers before they can use this application through a prominent pre-first use disclosure. Additionally, Verizon Wireless licenses location-based service Application Programming Interfaces ("APIs") to third-parties for incorporation of location-based services in third-party applications and services, such as weather applications or restaurant and movie guides, but only pursuant to our third-party contracts with developers requiring them to use location information only after receiving affirmative consent from customers (as well as compliance with all relevant laws, regulations, and industry standards). Moreover, Verizon Wireless tests the applications and services for, among other things, compliance with the contractual requirements.

Verizon Wireless provides detailed notice to our customers about the information collected from or about them and how it is used. Our privacy policy, available at

http://www22.verizon.com/privacy/, explains how customers' information (including location) is used to operate our network, provide our products and services, bill our customers, complete transactions on our network, identify fraudulent activity, analyze and improve performance metrics, and to comply with court orders, law enforcement requests, or emergency calls to 911.

With that overview, following is a more detailed explanation of some of the specific mechanisms and means through which Verizon Wireless provides our customers with control over the use of their location information. As explained below, we obtain our customers' affirmative consent before we use or share personally identifiable location information for commercial purposes, such as marketing offers to them within applications based on their location.

- **"On Device" Location Privacy Settings** – As illustrated below, and described above, Verizon Wireless requires device manufacturers and operating system providers to ship devices with the general location settings in the main menu turned off with respect to Verizon Wireless location-based services, and encourages these devices to be shipped in the off position with respect to third-party location based services that Verizon Wireless does not control. For example, we require that Verizon Wireless location based services are always turned off when the device is sold to the customer. This requires customers to affirmatively turn their location settings on by checking a box before any Verizon Wireless applications and services (or third-party applications and services) can use Verizon Wireless offered location-based services on devices. Customers can always revisit the location settings screen to review and change their selections. An example from an Android-based device is shown in the following screen shot:



- **"Location On" Icon** – Verizon Wireless devices sold since approximately 2006 have a satellite location icon that appears as an image in the menu bar at the top of device screens when devices are in "location on" mode and a customer's location information may be collected by applications and services available on the devices. This means that customers will be able to quickly determine whether their location setting is turned on and accessible by location-based applications and services. For example, the following Location On icon - - appears in the menu bar on most devices to tell customers that their devices are in "location on" mode. Similar icons may appear on other devices that do not use this specific image depicted above.

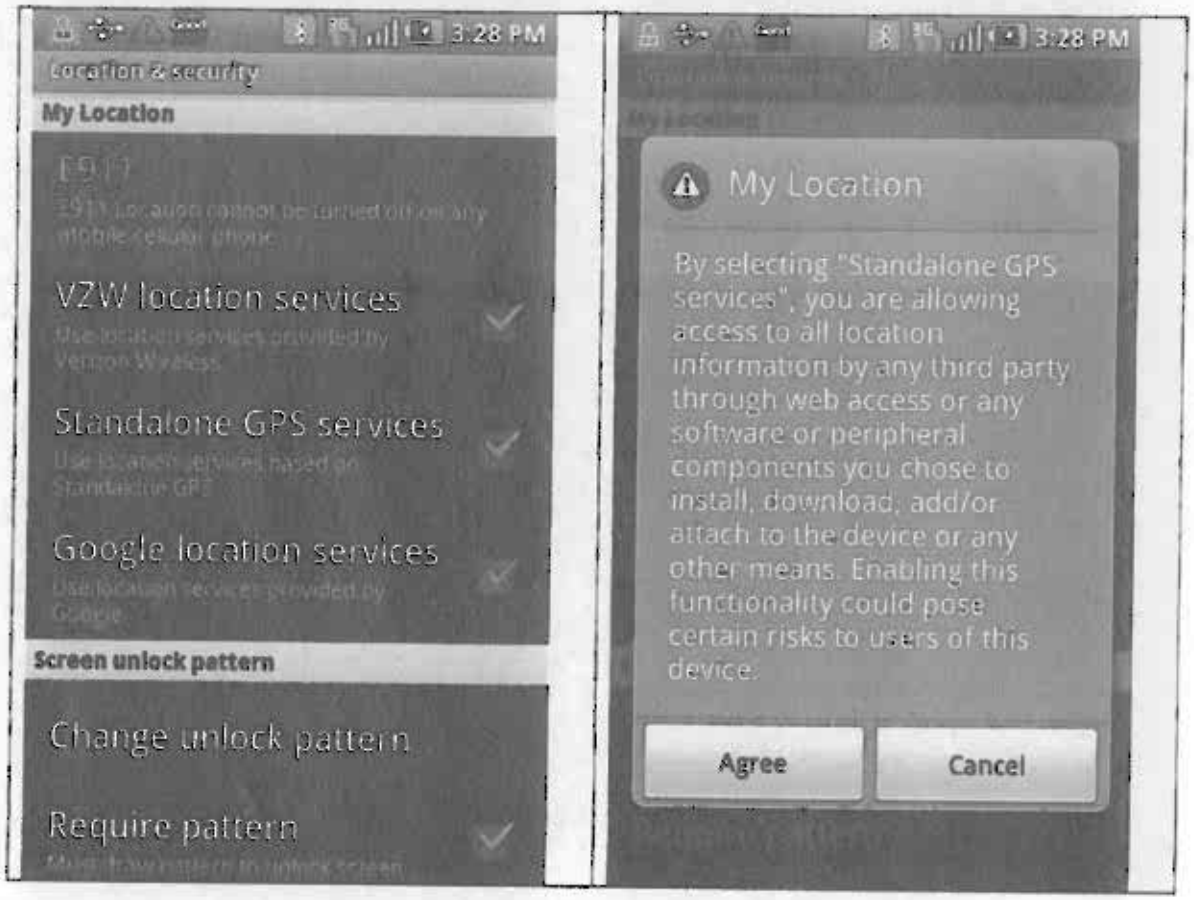
- **Location-Based Services APIs ("LBS APIs")** – Device manufacturers, application developers, and device operating system developers can access location information about Verizon Wireless customers through two mechanisms: (i) Verizon Wireless provided LBS APIs; and (ii) third-party provided LBS APIs. We discuss each below.

  (1) **Verizon Wireless Provided LBS APIs:** Verizon Wireless currently offers its own proprietary LBS APIs to third-parties to permit access to customers' location information. Access to this information can be obtained through two distinct technologies known as "Assisted GPS (which has the ability to provide a more precise location fix for a customer) or "Network Cell ID" data (which affords access to a more generalized location radius). Before allowing any such access,

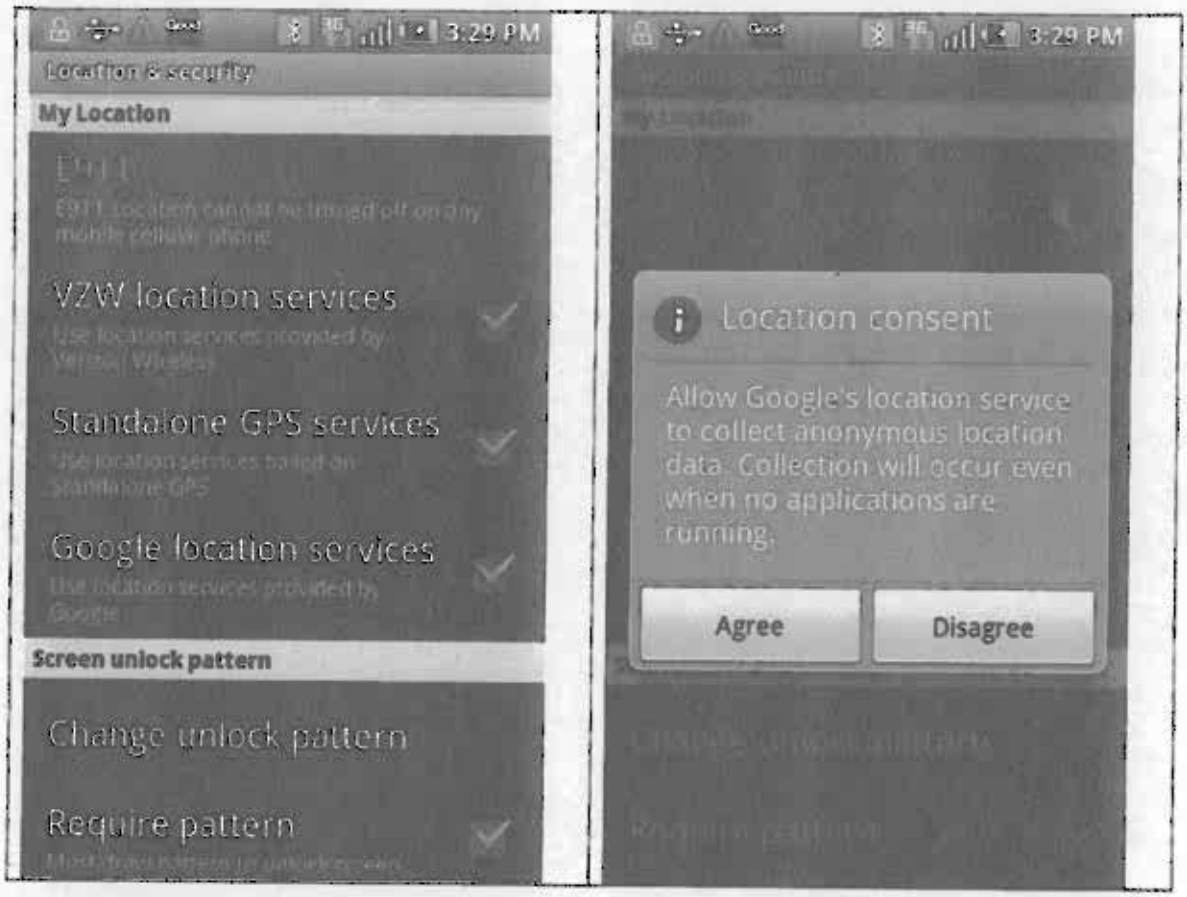
however, third parties must address privacy with clear disclosures requiring customers to affirmatively consent prior to the that third party's collection of the location information. More specifically, before allowing third parties to use its LBS APIs, Verizon Wireless: (a) requires third parties, for example developers submitting applications to Verizon Wireless' "V CAST Apps Store," to agree to terms and conditions that require compliance with the above privacy consent requirements; and (b) utilizes additional technical means to authenticate, validate, and authorize applications and services *prior to permitting third-party access* to customer location information. Therefore, any customers subscribing to third-party applications or services utilizing Verizon Wireless LBS APIs must agree to and have control over the collection and sharing of their location information through on-device consent options and settings, which they can view and modify. In addition, any specific applications and services that utilize Verizon Wireless LBS APIs must first obtain the customer's affirmative consent prior to download of the application. For example, Verizon Wireless requires that application developers incorporate the following disclosure before a consumer can download an application utilizing Verizon Wireless-provided LBS APIs from the V CAST App store:

"This app uses location data. By using this app, you consent and permit Verizon Wireless to share your location with others. This is no representation, warranty or guarantee of accuracy, completeness or timeliness of any location data, product or service."

(2) **Third-Party Provided Location-Based Services APIs** – A second way that third parties can access a customer's location information is through independently provided third-party LBS API services, which use the device's standalone GPS or other technologies, as explained more below. Verizon Wireless does not control incorporation and utilization of these third-party provided LBS APIs into third-party provided applications and services, and customers have access to an enormous variety of third-party provided applications and services through the Internet and third party application stores (such as Apple's App Store and Google's Android Market). Technologies that utilize these third-party LBS APIs can vary widely and typically utilize on device standalone GPS, Cell ID, IP Address, or Wi-Fi signal strength technologies that the third-party LBS API provider independently accesses. Verizon Wireless does not control, limit, or restrict customer access to, or use of, third-party provided applications and services (including those that utilize third-party provided LBS APIs). Instead, customers use these LBS-based services at their own discretion. Given the heightened consumer concern about the collection and use of location information, however, Verizon Wireless where possible requires that its device OEM suppliers incorporate privacy protections affording customers control over the collection, use, and sharing of their location information by these third parties through features and tools available in the location settings menu of the device. For example, when a customer selects the "Standalone GPS Services" box on Android devices, the customer is presented with the following affirmative consent screen, in response to which the consumer must click "AGREE" to authorize the location data collection:

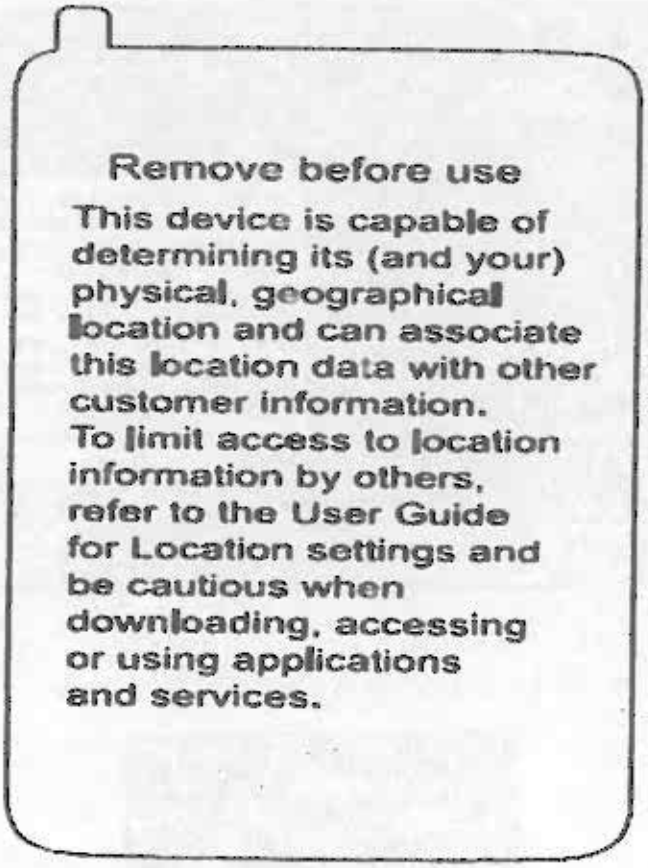


Customers using Google location services on Android operating system devices that are sold by Verizon Wireless receive the following disclosure and customer control mechanism:

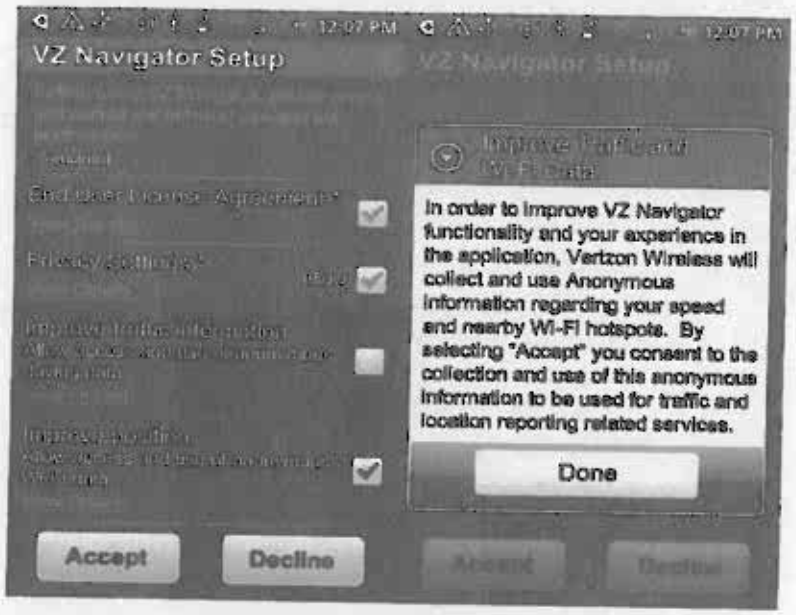


Accordingly, before the device can use these Google location services, the customer must click the "AGREE" button, and they can always navigate back to this screen to withdraw their authorization.

In addition, Verizon Wireless soon will begin to include the following notice as a removable sticker on the screen of all new devices it sells:



- **Verizon Wireless Provided Applications Using Location** – Verizon Wireless' applications and services provide clear notice to customers and allow them to control the use of location information. For example, users of the VZ Navigator application receive the following disclosure and consent screens before location information may be utilized for additional commercial purposes:



Users of VZ Navigator also can control their location settings as shown below:

- **My Verizon Account Privacy Settings** – Verizon Wireless customers also can control their location privacy settings on the Location Management website, which is accessible through their My Verizon online account website. Customers are able to view and edit their location settings for Verizon Wireless supported location-based services to which they subscribe. For example, the Location Management website allows customers to, among other things, specify if and when a service using Verizon

Wireless-supported location based services can access their location information. Customers can also download the free "Location Management" application from Verizon Wireless, allowing them to specify on their device if and when Verizon Wireless-supported location services can access location information on their device.

- **Additional Sales and Marketing Materials** – Verizon Wireless also provides the following important notice about the collection, use, and sharing of location information to customers in our consumer brochure, on our website (www.verizonwireless.com), and as reminders in "Bill Messages" to customers:

  "Your wireless device can determine its (and your) physical, geographical location ("Location Information") and can associate Location Information with other data. Additionally, certain applications, services and programs are capable of accessing, collecting, storing and using Location Information and disclosing Location Information to others. You should use caution when determining whether or not Location Information should be made available to others and you should review any applicable third party privacy policies before providing access. To limit potential unauthorized access to your Location Information, Verizon Wireless phones are preset to E911 only, which will only allow emergency response personnel to locate you if you dial 9-1-1 from your phone. Other wireless devices (such as Broadband Data Cards or devices without a keypad or user interface) may or may not have such limitations and location settings available. By enabling location settings you are permitting third party access to Location Information through software, widgets or peripheral components you choose to download, add or attach to your wireless device or through web access, messaging capabilities or other means and you are authorizing Verizon Wireless to collect, use and disclose your Location Information as appropriate to provide you with any location services that you enabled."

Each year, Verizon Wireless files an annual CPNI Certification with the FCC, providing its annual statement of compliance pursuant to Section 64.2009(e) of the Commission's rules. This annual Certification provides information regarding the safeguards and training implemented by Verizon Wireless to ensure that CPNI information is only accessible and used with proper customer consent, depending upon the specific information and the intended type and form of use. Verizon Wireless has an extensive training program that informs all employees, including sales, marketing and customer service personnel, about the CPNI rules and regulations and notifies them that any failure to comply with company policy is a serious violation and may result in disciplinary action, up to and including termination of employment. The Verizon Wireless employee Code of Conduct ("Code") defines CPNI and requires compliance with Verizon Wireless' CPNI safeguards. Verizon Wireless trains all new hires on the Code at the time of hire and trains all employees on the Code periodically. Verizon Wireless also trains all new hires on Keys for Safeguarding Privacy and Customer Information at the time of hire.

Verizon Wireless' Office of Integrity and Compliance has primary responsibility for drafting, disseminating, and training on the Code. It also maintains a confidential 1-800 number for employees to report actual or possible violations of the Code, including violations relating to customer privacy. Employees are advised of the 800 number via the

Code, postings in the workplace, periodic e-mail alerts on our intra-net site "VZ Web" to all employees, the distribution on a quarterly basis of an internal compliance newsletter called *Integrity Times*, which addresses a myriad of ethics and compliance issues, particularly around privacy and protecting customer information, as well dissemination of methods and procedures for using CPNI.

2. ***What personally identifiable information does your company collect from its customers?***

When a customer enters an agreement with Verizon Wireless or contacts us with service inquiries, we collect information from the customer to complete their order, communicate with them, and provide and bill for the service. This is explained in our privacy policy:

> ***"When you place an order for Verizon products or services, we collect information from you that we use to deliver, provide, confirm, change, bill, monitor, and repair those products or services and to resolve issues with your order or with our products and services. The information we collect may include your name and address and the telephone numbers and email addresses where you may be reached, as well as Social Security Number or payment information necessary to establish credit or set up billing. We also use this information to establish your customer account, maintain a record of the products and services you buy from us, and maintain billing records for your account. We may use your address, e- mail address, and phone number information to contact you about products and services that we offer."***

We also collect and use information from customers when they use our products and services. We use this information for operational and transaction purposes, as explained in our policy:

> ***"Transactional Information: We collect information about your use of the products and services we offer. Information such as call records, service usage, traffic data, service options you choose, and other such information you provide may be used for billing purposes, to deliver and maintain products and services, or to help you with service-related issues or questions. This information also may be used for other purposes such as providing you with information about product or service enhancements, determining your eligibility for new products and services, and marketing to you based on your use of the products and services you already have, subject to any restrictions required by law. This transactional information also may be used to help us improve our services; research and develop new products; provide and offer promotions and service offerings; and protect our networks, services and users from fraudulent, abusive, or unlawful uses."***

3. How is this information collected (i.e., initial sign up process, usage of mobile phone, etc.)?

As explained in greater detail in response to Question 2, personally identifiable customer information is collected during the initial sign-up process with Verizon Wireless, and when customers use our services and complete transactions (such as buying ringtones and applications), interact with our website, or make customer service inquiries. We also purchase lead lists and demographic information about our customers from third parties.

4. [a] How does your company use customer's personally identifiable information?

As explained in greater detail in response to Questions 1 and 2, customer information is used to provide and maintain our services and operations and to complete our customers' transactions when using our network and wireless devices we provide. We may also market products and services using customers' personally identifiable information; for example, to send them an e-mail or text message with information about a new device or service, but Verizon Wireless does not use location information that is linked to personally identifiable information for marketing purposes unless affirmative consent is obtained from the customer.

[b] Does your company rent or sell the information?

No. Verizon Wireless does not rent or sell its customers' personally identifiable information. In the event we decide in the future to share such information, it would only be with customers' meaningful consent that takes into consideration the particular use and form of the information at the point when it would be shared with a third party. Because of our commitment to open platforms and the requirements of the C Block rules, Verizon Wireless also cannot control the extent to which third-party applications and services may collect, use, or sell information that may be collected from the applications or services independently downloaded or used by customers on their devices. That is why, as mentioned above, we warn customers to be especially careful when accessing third-party products and services not provided by Verizon Wireless.

[c] Does your company use personally identifiable information for marketing purposes?

Yes, Verizon Wireless uses personally identifiable information about our customers or potential customers to market its own products and services, as more fully described in response to Questions 2 and 4. Verizon Wireless presently does not market its own or third-party offers to customers, nor does it authorize third-parties to market

their own products and services, based upon customers' personally identifiable location information unless affirmative consent is obtained from the customer.

5. ***[a] How does your company store this information (i.e., in a form that is encrypted or otherwise indecipherable to unauthorized persons)?***

Verizon Wireless employs robust privacy protection practices because we value customers' expectations of privacy, and our reputation for trust is an important business imperative and competitive asset. The protection of the data entrusted to us by our customers is an integral part of the Verizon Wireless culture and is engrained in our business practices and policies. As a company, Verizon Wireless goes to great lengths to ensure sensitive personal information pertaining to our customers is only available to authorized persons. Verizon Wireless' corporate policy outlines the privacy protections that must be in place for sensitive personal information, including encryption requirements when appropriate based on the sensitivity of the data and the potential risk. Contract provisions with third party vendors who may receive Verizon Wireless customer data in support of business processes contain data protection requirements that align with internal requirements. Additionally, to ensure that customer personally identifiable information is protected from unauthorized persons, systems that store customer information require employees to provide valid credentials which are assigned based on such employees having a valid business need to access that data. Access to more sensitive personally identifiable information (such as social security numbers, birth dates, driver license numbers, and credit card information) is restricted even further to a very limited subset of employees that may have a need to know this information for Verizon Wireless to operate its business.

[b] How long is it stored?

The Verizon Wireless record retention periods vary depending upon the business need, the type of data, the location of the data, the technical and operational issues associated with retaining the data, and the myriad legal requirements (including statutory law, law enforcement requirements, and document retention obligations in the context of civil litigation) to retain various types of documents that contain the data. Verizon Wireless maintains records management and retention requirements outlining the length of time that customer information is to be retained. In general, customer account and billing information is retained for a period of seven years from collection to support business obligations such as customer disputes, corporate or fraud investigations, legal proceedings, auditing, operational planning, and taxation. As noted above, exceptions to this retention policy are made based on a valid business reason (such as pending litigation or a government investigation) or when otherwise required by law.

[c] How does your company dispose of this information?

Verizon Wireless policies outline data destruction requirements based on the nature of the data and the storage media used. For example, paper-based documents containing sensitive customer information must be shredded and server hard drives must be rendered unreadable or unrecoverable. These policies also address other storage

media including portable devices like CD's, diskettes, and USB drives as well as printers, copiers, or fax machines with internal memory capability.

[d] Is the information always disposed of after a customer has terminated his or her business relationship with your company?

The retention of information pertaining to former customers of Verizon Wireless is managed in accordance with corporate records management and retention practices (see answer to Question 5[b]). This information is maintained for a period necessary to support business and legal obligations. These obligations include supporting data requests from former customers, regulatory inquiries, credit reporting, and litigation matters. In general, personally identifiable information of former customers is disposed after 7 years. Customers and former customers have the ability to choose that Verizon Wireless not use their information for certain marketing purposes (e.g., direct mailings, emails, and calls) and may inform Verizon Wireless that their information should not be shared with affiliates at any time.

[e] If not, why not?

Please refer to our answers to Question 5[b] and 5[d].

6. ***[a] Other than pinpointing a customer's location for purposes of identifying the strongest signal, does your company use any other mechanisms for determining the location of a customer's mobile phone, such as how frequently the customer checks her email?***

Please refer to our answers to Questions 1, 2, 3 and 4. More specifically, Verizon Wireless does not monitor how frequently customers check e-mail. Beyond the mechanisms discussed above, Verizon Wireless must collect information about mobile devices using its network as they change location and interact with the wireless network. Collected data includes, among other things, which tower or antenna a device is connected to, what state the device is in, how far it is from the closest tower, how strong the signal is at both the tower and the device, as well as other information (such as signal strength and device type). This data is collected so that Verizon Wireless can ensure that its customers' devices have the right coverage and signal to make a phone call or to transmit data across very geographically diverse and complex networks maintained by Verizon Wireless and third-party roaming partners. The data collected relates to the device, such as the device's phone number or serial number, and not an individually identified customer. That information is associated with a customer's personal information only when necessary for a very specific purpose, such as billing, handling of disputes, and law enforcement or emergency purposes. This information is also used to troubleshoot network issues, such as dropped calls, ineffective voice or data attempts, and network signaling issues. This raw data and information collected by Verizon Wireless' network is not in the form of latitude and longitude of devices. Instead, it is collected in a form that is associated with what tower devices are connected to, on what cell sectors,

and at what times. Verizon Wireless' ability to identify the precise location of a device is limited to authorized employees who have access to the data needed to track or locate a specific device on our network, which generally speaking, is only done when Verizon Wireless has been served with proper legal process to assist law enforcement, public safety answering points, and/or search and rescue teams when an emergency involving death or serious physical injury to any person requires disclosure of information without delay.

[b] If yes, what are these mechanisms and what is the purpose of each of them?

Please refer to our answers to Question 1, 2, 3, and 4.

7. ***[a] Is it a common practice of your company to inform the customer when relevant data is being collected and how long this data is being used? [b] If not, why not?***

Yes, it is a common practice for Verizon Wireless to inform our customers when personal information is being collected about them, under both our privacy policy and our specific service disclosures and notices, except as otherwise forbidden by law. As stated in our privacy policy, Verizon Wireless apprises customers that we maintain sensitive records only as long as necessary for business and legal needs. The privacy of consumer information is an important consideration in the design of our products and services. We are also committed to educating our customers about how they can protect their personal information. For example, we recommend that customers always:

- Use caution and discretion when determining whether or not to utilize location-based services, including whether location data should be made available to third parties;
- Carefully review the privacy policies of the application providers and third parties who are seeking access to location data;
- Check their mobile device and privacy settings periodically to ensure the setting is what they want;
- Only use software, widgets, peripheral components, and Internet access or other services from reliable sources; and
- Use the "911" default location setting to limit access to location data when commercial location-based services are not in use.

Verizon Wireless also adheres to CTIA Best Practices on Location Based Services.

In sum, the meaningful privacy choices that Verizon Wireless provides our customers, as well as the ongoing efforts we make to secure and protect customers' personal information, as described in this letter, provide robust privacy protections for our customers' personal information.

Sincerely,

Peter B. Davidson