at&t

Robert W. Quinn, Jr.
Senior Vice President
Federal Regulatory and
Chief Privacy Officer

AT&T Services, Inc.
1120 20th St., NW, Suite 1000
Washington, DC 20036
T: 202 457.3851
F: 202 457.2020

April 19, 2011

The Honorable Edward Markey
Co-Chair
House Bi-Partisan Privacy Caucus
House of Representatives
2108 Rayburn House Office Building
Washington, DC 20515

The Honorable Joe Barton
Co-Chair
House Bi-Partisan Privacy Caucus
House of Representatives
2109 Rayburn House Office Building
Washington, DC 20515

Dear Congressmen Markey and Barton:

I am responding to your letter to Randall L. Stephenson, Chairman, Chief Executive Officer and President of AT&T Inc., related to a recent article in the New York Times concerning the collection and use of location information by Deutsche Telecom for one of its customers, Mr. Malte Spitz.

AT&T has long recognized the sensitive nature of wireless location information and, as set out in detail below, has established policies and procedures for the collection, use and storage of that information. In November of 2010, we posted an update to our Privacy Policy[1] that significantly expanded on our FAQ section devoted to Location Information – providing additional information on what location information is, how it is collected, how we use it, what Location Based Services are, where and how they may be obtained, how they work, and confirming our commitment to providing prior notice and obtaining consent for the use of that information. In short, providing transparent notice to customers about our collection and use of personal information – including wireless location data – is fundamental to our privacy practices, and to the trust our customers place in us.

AT&T is committed to working with industry and policy makers to improving the privacy protections available to users of wireless devices, and actively participated in the development of

[1] This update was posted on November 18, 2010 for customer feedback, and became effective on March 1, 2011. A copy of the AT&T Privacy Policy is Attachment A to this letter.

the CTIA Best Practices and Guidelines for Location-Based Services. As noted in that document and discussed below, wireless carriers are only one of many sources of location information, and only one of many participants in the provision of location-based services to end users.

In light of the NYT article on wireless location data that led to this request, we provide our responses to your questions about AT&T's customer data collection, storage and disclosure practices with a particular focus on wireless location information.

1. **Please describe the policies and procedures you 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.**

Section 222 Compliance

The policies and procedures utilized by AT&T to comply with § 222 are disclosed in detail in AT&T's annual officer compliance certifications, filed with the FCC pursuant to the requirements of 47 C.F.R. § 64.2009. AT&T's certifications for the calendar year 2010 were filed on March 1, 2011 (see Attachment B).[2]

AT&T does not use, disclose or permit access to individually identifiable call location information for any purpose other than providing the underlying telecommunications service from which the information is derived, or services used in the provision of such telecommunications service. If AT&T were to use, disclose or permit access to individually identifiable call location for any other purpose, it would do so only with the express prior authorization of the customer as required by § 222.

AT&T Data Services

AT&T also derives individually identifiable location information from data services. Data Services are not telecommunications services, and are not subject to the requirements of § 222. However, AT&T provides notice to and obtains consent from its customers prior to using that information for any commercial purpose other than as necessary to provide the underlying service to the user.

AT&T's policies and practices in this area are set out in the AT&T Privacy Policy. In particular, AT&T's responses to the Privacy Policy FAQ on Location Information (beginning on page 12 of Attachment A) provide considerable detail concerning AT&T's use and collection of wireless and other location information.

[2]These certifications are publicly available on the FCC's website at http://fjallfoss.fcc.gov/ecfs/document/view;jsessionid=NJQLsMv1G7YYwZQBhmVkTnqn3vZ1lzmyc5wtG9BmHnPLM3XSXn2d!942891741!1055465516?id=7021032838

Third-party Application Developers & Location Aggregators

Network providers like AT&T are only one of many potential sources of location information, and only one means by which customers may obtain Location Based Services ("LBS"). In recognition of the sensitivity of location information, the number of participants that can and do play significant roles in the delivery of LBS to users, and the need to ensure protection of the customer's privacy, AT&T and other CTIA members collaborated in the development of the CTIA Best Practices and Guidelines for Location Based Services. These Best Practices are founded on two fundamental principles: LBS providers must ensure that users receive meaningful notice about how location information will be used, disclosed and protected, and they must ensure users consent to such use. They provide illustrations of who is or is not an LBS Provider with obligations under the Best Practices, as well as guidelines on providing notice, obtaining consent and securing customer location information.

As set out in the AT&T Privacy Policy, when AT&T is the LBS provider customers will receive prior notice and must give their consent before their location is used or shared. However, there are situations in which AT&T has no role in the provision of LBS to the customer, and therefore, plays no role in providing notice or obtaining consent. For example, AT&T customers may download LBS applications from third-party sources that are not in any way affiliated with AT&T. Those providers may derive the location of the customer's device directly from the handset, or may obtain it by partnering with location providers who, in turn, obtain location from use of GPS, Wi-Fi hotspot mapping, reverse-engineered cell tower ID information, and other available mechanisms. The location information available through these sources is not obtained from AT&T (or any other wireless carrier), but is every bit as detailed and comprehensive as any carrier information. And, in these cases, AT&T has no control over or involvement in providing either the application or the location information used by the application.[3]

There also are situations in which AT&T is not the LBS provider, but has some role in providing the location information used in connection with a third-party LBS. While not strictly obligated to do so under the CTIA Best Practices, in those situations AT&T nonetheless has undertaken measures designed to ensure the provider is following CTIA guidelines. For example, AT&T requires non-AT&T application developers that sell or provide their applications through the AT&T AppCenter to comply with the CTIA guidelines and with AT&T's own Location-based Services Privacy Guide,[4] including disclosure of:

---

[3] Communication between cell towers and handsets is fundamental to the provision of cellular service. Cell towers broadcast their Cell ID numbers, which are recognized by the handsets within their broadcast areas. The handsets relay these Cell ID numbers, together with the associated signal strength and other related information, back to the network. Using that information, the network determines which cell tower is the best serving tower for the handset. The Cell ID information and GPS coordinates on the handset can be retrieved by third-party applications (resident on the handset) and transmitted back to third-party servers. Using this Cell ID and GPS coordinate information, these third parties have created comprehensive databases of wireless carrier Cell IDs and associated coverage areas, which they can use to determine user location without any involvement by wireless carriers.

[4] Attachment C.

- what location information is collected;
- how the location information will be used;
- the identity of the collecting party and whether location information is shared with third parties; and
- the security measures put in place to protect the location information.

AT&T also prohibits those developers from:

- accessing location information unless a request is first initiated by the user;
- unilaterally initiating a LBS or accessing location information directly or through the developer's API's; and
- Storing location information any longer than necessary to provide the LBS.

During the application review process before third-party applications are made available through the AT&T AppCenter, the developer is required to divulge whether the application collects or uses location information. Applications that do so are further reviewed to confirm that they meet the requirements of AT&T's Location-based Services Privacy Guide. AT&T makes network-based location information available to trusted third-party Location Aggregators. As the name implies, Location Aggregators have access to such information not only from AT&T, but from other network and non-network providers as well. They use that information to provide location information to LBS providers. In this arrangement, the LBS provider remains the entity with responsibility under the CTIA guidelines for providing notice and obtaining consent of the user. While AT&T has no direct control over the LBS provider in this situation, AT&T requires that the Location Aggregators with which it does business ensure that any third-party developers with access to AT&T Location information through the Aggregator agree to the protections and provisions for notice and consent set out above.

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

The term "Personal Information" is defined in the AT&T Privacy Policy as "information that directly identifies or reasonably can be used to identify an individual customer. Examples include name, address, telephone number, e-mail address, Social Security number, and financial account number." We consider any information fitting this definition – including location information – to be "personally identifiable." Additional information about the personal and non-personal information collected by AT&T can be found in response to the Privacy Policy FAQ "What information do we collect?" on page 8 of Attachment A.

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

Location information is collected when a customer uses a Location Based Service, and may also be collected for network performance and improvement purposes, as discussed in response to Question 6 below. Additional information about how AT&T collects information is provided in response to the Privacy Policy FAQ "How do we collect information?" beginning on page 8 of Attachment A.

4. **How does your company use customer's personally identifiable information? Does your company rent or sell the information? Does your company use personally identifiable information for marketing purposes?**

   AT&T uses wireless location information to provide customers with wireless voice and data service, as well as to maintain and improve our network and the quality of our customers' experience.

   AT&T will not sell customer personal information to anyone, for any purpose. Period. This is a fundamental commitment we have made to everyone who has a relationship with AT&T and it is central to how we do business every day.

   We may use personal information for marketing purposes, subject to the commitments we have made in the AT&T Privacy Policy – including those that apply to the use of location information as discussed above and the CPNI requirements of §222. Additional information about our use of the information we collect is provided in response to the Privacy Policy FAQ "How do we use the information we collect?" on page 9 of Attachment A.

5. **How does your company store this information (i.e., in a form that is encrypted or otherwise indecipherable to unauthorized persons)? How long is it stored? How does your company dispose of the information? Is the information always disposed of after a customer has terminated his or her business relationship with your company? If not, why not?**

   Location information is stored on a variety of AT&T systems and platforms used for the provision of services, to manage billing and other related business purposes.

   AT&T's security policies require that information classified as Sensitive Personal Information or "SPI" be encrypted. Longitude and latitude coordinates in combination with a Mobile Station Integrated Services Digital Network Number (Mobile Station ISDN or MSISDN) or when associated with a customer name or accompanied by any other SPI data element (such as date of birth, SSN, Credit Card Number; government issued ID numbers) is classified by AT&T as SPI. In 2009, AT&T established a comprehensive program to identify occurrences of SPI in our corporate databases and encrypt that SPI data according to our security policies. That program is targeted to complete by the end of 2012. Once the overall project is completed, any SPI that remains unencrypted because of technical or business issues (such as systems pending retirement or system changes) will be managed by our security risk process until those remaining occurrences can be encrypted or deleted.

   Encryption is only one element in AT&T's comprehensive program of electronic and administrative safeguards designed to secure the information we collect, to prevent unauthorized access to or disclosure of that information and to ensure it is used appropriately. See Attachment D for more detail about AT&T network safeguards relevant to this inquiry.

In addition to these protections, the AT&T Code of Business Conduct requires all employees to follow the laws, rules, regulations, and court and/or commission orders that apply to our business — including, specifically, the legal requirements and company policies related to the privacy of communications and the security and privacy of customer records. Employees who fail to meet the standards embodied in the AT&T Code of Business Conduct are subject to disciplinary action, up to and including dismissal. AT&T personnel receive regular training to reinforce the company's standards of confidentiality and security.

As stated in the AT&T Privacy Policy, we retain the personal information of our customers and users "as long as needed for business, tax or legal purposes, after which we destroy it by making it unreadable or undecipherable." Depending on the system or service platform involved, location-related information may be retained for as little as several days (as when a server is simply written over during the course of providing service) or as long as five years (as in the case of Call and Data Detail Records, which are used for billing purposes). And, of course, information will be retained as necessary to comply with legal process.

AT&T retains the information of both current and former customers according to this policy. Among other reasons, the information of former customers may continue to be necessary for billing purposes and for fraud investigations, to facilitate the establishment of accounts for former customers who return to AT&T, and to ensure compliance with legal hold requirements.

6. **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 e-mail? If yes, what are these mechanisms and what is the purpose of each of them?**

AT&T uses a number of technologies to determine the approximate location of a mobile customer's mobile device.

First, to be clear, AT&T does not "pinpoint a customer's location" for the purpose of identifying the strongest signal. Rather, when the customer uses her wireless device for non-Location Based Services (e.g., to make a voice call, check email or browse the web) the AT&T network registers the identification number of the cell tower serving that customer (referred to as the Serving Cell ID). Serving Cell ID is the only location-related information necessary for voice and non-location based data services. No latitude and longitude coordinates for the tower are identified, and no triangulation or other calculations are used to locate the individual customer. [5]

However, when a customer utilizes a location based service (as with 411, 911, a "friend locator" application or a navigation/mapping application), more precise information about location is needed for service delivery. To provide such services, AT&T may use one or

[5] Serving Cell ID alone is not sufficient to locate an individual. However, Serving Cell ID can be readily associated with the latitude and longitude of the tower location when necessary to provide the underlying location based service as described under the heading "Basic Cell ID."

more of the following technologies to determine the approximate location of a customer's wireless device:

Basic Cell ID: This method associates the serving cell ID together with the lat/long of the tower and information about the coverage of the wireless antenna on the tower and estimates that a given user will be located in the middle of that coverage area. This method is very fast, and can be used to determine the approximate location of any device type on the network, but not very accurate (typically within 1000 meters for urban areas, 10,000 or more for rural).

Enhanced Cell ID: This method utilizes the same information as Basic Cell ID, but also incorporates radio frequency parameters (such as timing advance and neighbor cell measurements) to the calculation logic. This method provides a greater degree of accuracy than Basic Cell ID (within 500 meters for urban areas, 9,000 for rural).

Assisted GPS (A-GPS): With this method, the AT&T network sends GPS assistance data (a file of data related to the location of the serving cell tower and the nearest satellites) to the user's handset, where it assists the GPS chip to more rapidly identify the most appropriate satellite for the GPS to use to locate a given device. This method is more accurate than either Basic or Enhanced Cell ID (approximately 15 to 30 meters), but also is slower and does not work well indoors.

The location method used by AT&T in connection with a given Location Based Service is based on the needs of a requesting application. Applications that require a high degree of accuracy and are not dependant on fast return may use A-GPS, while those that require a faster response and are not accuracy dependant might use Basic Cell ID.

In addition to the location technologies listed above, AT&T uses Signal Timing-Based Location Technology to assess network performance experienced by AT&T customers. With this method, wireless location is estimated based on timing differences in radio signals sent from cell towers to wireless devices. Using this method, AT&T is able to gather network performance information, including the approximate location of network events (such as dropped calls) for network improvement purposes.

AT&T also uses network improvement applications on handsets (like AT&T Mark the Spot) to collect network performance information and to determine the approximate location of a wireless device at the time a network event is experienced. Those applications use AGPS technology to determine location.

In the future, location information derived from Signal Timing-Based Location, and from network improvement applications may be used to provide LBS and other location-related services to our customers, subject to our Privacy Policy commitments to notice and consent.

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

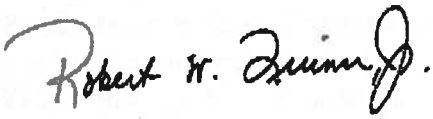
   Yes. Transparency about the information that AT&T collects and how we use, share and protect that information is one of the guiding principles on which our Privacy Policy is based. We provide transparent notice of our data collection practices through our Privacy Policy, which is written in clear and easy-to understand language. Following the CTIA Best Practices, we also will provide specific notice about the collection of location information by an AT&T LBS when we believe that additional, separate notice and consent is appropriate for the type of application involved.

   For example, the AT&T FamilyMap application provides customers with the ability to conveniently locate a family member's mobile phone from another wireless phone or from the Internet browser on a customer's computer. The service is limited to lines on the same wireless account. When a customer first seeks to establish service through the FamilyMap application, a temporary password is sent to their device. This temporary password, which is used to set up the service, is designed to protect against unwanted location tracking by helping to ensure that the person requesting the service actually has a device registered on that account and is authorized to set up the service.

During the sign up process, the account holder is presented with marketing disclosures and an End User Licence Agreement that clearly and conspicuously state that the application collects and uses the location information of the selected wireless phones. An SMS message is sent to all wireless devices on the FamilyMap account alerting users that they can be located by another phone number on the account. In addition, the account holder receives a welcome letter (see Attachment E) and an email message (if the email address is on file) advising that the FamilyMap application will locate the selected devices, and providing information on how to access location privacy tools for the management of the privacy preferences of those on their account. And, as an additional protection, AT&T sends periodic notices to all wireless phones registered on the FamilyMap account, reminding them that they are able to be located via the application. See Attachment F for screen shots of the sign up notifications, as well as the SMS notices sent to the wireless devices.

Thank you for the opprtunity to provide you additonal information regarding AT&T's Privacy Policy and the information we collect on our subscribers. We trust that the information we have provided will be of assistance in your inquiry. Please feel free to contact me with any additional questions that you might have with regard to AT&T's policies.

Sincerely,



Robert W. Quinn, Jr.
Sr. Vice President-Federal Regulatory &
Chief Privacy Officer

Attachments