

result in the collection or use of location information. With informed customer consent, the promise of location-sensitive wireless services will be realized.

Accordingly, pursuant to Sections 1.49, 1.52 and 1.401 of the Commission's rules, CTIA respectfully requests that the Commission promulgate rules to ensure that mobile customers (1) are well informed of location information collection and use practices *prior* to collection; (2) have a meaningful opportunity to consent to the collection and use of this information for location-based services; and (3) are assured of the security and integrity of any collected location information. These rules should provide a safe harbor for any location information service provider that ascribes to these privacy principles. And finally, the rules should be technology neutral so that the mobile consumer's privacy expectations are satisfied no matter the type of mobile device or the roaming market in which it is used.

I. BACKGROUND – THE WIRELESS WORLD

CTIA displays a counter on its web site showing the daily growth of U.S. wireless subscribers.² Each day, the number increases by 45,924 new wireless subscribers, one every two seconds. There now are over 105,931,662 U.S. wireless subscribers. Experts estimate that by 2005 there will be over 1.26 billion wireless phone users around the world. We can now say that it truly is a wireless world.

Moreover, wireless and the Web are converging. Mobile commerce is expected to grow at seemingly incredible rates as mobile users access the Internet and the enterprise from a multiplicity of devices ranging from cellular phones to personal digital assistants. Not only does mobile computing offer convenience, but it ushers in an era of

² See www.wow-com.com.

new services and applications based on the ability of the service provider to locate or establish the presence of the accessing device.

Location-based services allow mobile users to receive services based on their geographic location, position or known presence. The Commission is most familiar with location service enabling technologies through its Enhanced 911 docket.³ The new technologies that allow a wireless phone user to be located in the event of an emergency also will enable a host of new commercial applications.

Thus, through both network- and handset-based technology,⁴ a subscriber to a location service can access driving directions, local news or weather, traffic delay updates, so-called “concierge” services to make dinner reservations or purchase theatre tickets, or access directory services.⁵ The delivery of information, communications and entertainment to in-vehicle and mobile devices, known as “telematics,” is enjoying tremendous growth and interest as more location-based services become available.⁶

Similarly, through location-based systems, Intelligent Transportation Systems (“ITS”) have the potential to make it possible for traffic management agencies to know

³ See Revision of the Commission’s Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, CC Docket No. 94-102, RM-8143, Notice of Proposed Rulemaking, 9 FCC Rcd 6170 (1994) and subsequent proceedings.

⁴ Network-based solutions rely on accessing information in a wireless carrier’s home location register to locate the mobile device. Handset solutions rely on global positioning system (“GPS”) information derived from a GPS chip in the handset and reported to the provider over the wireless network.

⁵ General Motor’s OnStar GPS system, for example, provides roadside assistance, concierge services and directions. See www.onstar.com.

⁶ See www.atxtechnologies.com.

where individuals travel, what routes they take, and travel duration.⁷ The public benefits from such services are enormous.

Finally, location-sensitive content, advertising and personalization services are being deployed today.⁸ Consumers will be able to receive relevant content when they want it and where they want it.

While all of these applications and services promise a wealth of consumer benefit, legitimate privacy concerns abound over fears of “location-based applications that allow [service providers] to track where users are and send them alerts about sales on travel or personal goods.”⁹ As a consequence, the Federal Trade Commission (“FTC”) will host a two-day, public workshop on December 11-12, 2000, to examine emerging wireless technologies and the privacy, security, and consumer protection issues they raise.¹⁰

CTIA strongly believes that privacy concerns regarding location information must be addressed if new services and applications are to be accepted by consumers. CTIA welcomes the discussion and has crafted a set of best location information principles to assure consumers that location information will be collected and used only as directed. CTIA invites the Commission to adopt these principles as part of its implementation of Section 222 of the Communications Act of 1934, as amended, and as the governing agency for commercial mobile radio services and other communications technologies.

⁷ See www.itsa.org.

⁸ See, e.g., www.airflash.com; www.viair.com; and www.adforce.org.

⁹ M. Hamblen, *Location information could invade privacy of wireless users, analysts warn*, www.computerworld.com/cwi/story/0,1199,NAV47_STO51388,00.html (quoting A. Davidson, Center for Democracy and Technology) (Sept. 28, 2000).

¹⁰ See <http://www.ftc.gov/bcp/workshops/wireless/index.htm>.

II. THE LEGAL FRAMEWORK FOR LOCATION INFORMATION

A. The Wireless Communications and Public Safety Act

As part of the Wireless Communications and Public Safety Act of 1999 (“WCPSA”), Congress deemed location information to be customer proprietary network information (“CPNI”) and therefore subject to certain limitations under the Communications Act of 1996.¹¹ Under WCPSA, with certain limited exceptions,¹² the user of a commercial mobile service or automatic crash notification system shall not be considered to have approved the use or disclosure of or access to call location information “without express prior authorization.”¹³

In addition to the express approval provision, as part of the overall CPNI framework, a telecommunications carrier must disclose location information to any person designated by the customer upon affirmative written request by that customer.¹⁴ Similarly, a telecommunications carrier may, without customer approval, use, disclose or

¹¹ Wireless Communications and Public Safety Act of 1999, Oct. 26, 1999, P.L. 106-81, § 2, 113 Stat. 1286.

¹² The exceptions are codified section 222(d) of Title 47 and permit use of CPNI to initiate, render, bill, and collect for telecommunications services; to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services; or to provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if such call was initiated by the customer and the customer approves of the use of such information to provide such service. WCPSA also added a location information specific exception to permit disclosure for emergency situations.

¹³ 47 U.S.C. 222(h)(1).

¹⁴ 47 U.S.C. 222(c)(2).

permit access to aggregate customer information that contains location information from which individual customer identities and characteristics have been removed.¹⁵

On August 24, 2000, the Commission took steps to implement the public safety aspects of the WCPSA but decided to defer consideration of the location information provisions to the pending CPNI docket.¹⁶

B. The Commission's Pending CPNI Docket

On May 17, 1996, the Commission initiated a rulemaking regarding the obligation of carriers under Section 222 of the Communications Act in regard to protecting customer proprietary network information (“CPNI”).¹⁷ The Commission released its CPNI Order on February 26, 1998.¹⁸ After numerous reconsideration petitions and revisions of the Commission’s Order, several carriers and interest groups challenged it on the grounds that the proposed CPNI restrictions violated the First Amendment.¹⁹

¹⁵ 47 U.S.C. 222(c)(3). Aggregate customer information under the Telecommunications Act is “collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.” 47 U.S.C. 222(f)(2).

¹⁶ In the Matter of Implementation of 911 Act, *Fourth Report and Order and Third Notice of Proposed Rulemaking*, CC Docket 99-105, WT Docket No 00-110 (Rel. Aug. 29, 2000) at par. 7.

¹⁷ In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information, Notice of Proposed Rulemaking, CC Docket No. 96-115, 11 FCC Rcd 12513 (1996).

¹⁸ Second Report and Order and Further Notice of Proposed Rulemaking, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, C Docket No. 96-115 (Rel. Feb. 26, 1998).

¹⁹ See *U.S. West v. FCC*, 182 F.3d 1224 (10th Cir. 1999), *cert. denied*, 147 L. Ed. 2d 248, 120 S. Ct. 2215 (2000).

Ultimately, the Tenth Circuit Court of Appeals held that the Commission's rules were unconstitutional, vacating the Order and remanding the matter to the Commission for further proceedings.²⁰ The Commission has not commenced further proceedings as of this date but has indicated that it intends to do so in the future.

CTIA respectfully urges the Commission to commence a separate proceeding in response to this petition rather than bundle the location privacy issue with other CPNI issues. The location privacy question is uniquely a wireless concern. CTIA expects that a broad range of commenters will be interested in this rulemaking that otherwise would have no interest in the general CPNI rulemaking. Further, it is in the public interest and the interest of emerging location service providers and consumers of such services to know the privacy rules as soon as possible.

III. LOCATION PRIVACY PRINCIPLES

CTIA's proposed privacy principles rely on well-established fair information practices.²¹ Thus, CTIA's privacy principles provide for notice, consent, security and integrity of information, and technology neutral rules.

²⁰ *Id.*

²¹ See *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress*, Federal Trade Commission, (May 2000) at 3-4. CTIA recognizes that the FTC ordinarily would view enforcement or some reliable mechanism to impose sanctions for noncompliance as an essential ingredient of a self-regulatory initiative. However, given the regulated environment in which carriers operate, such a provision is not necessary. Once adopted by the FCC, failure to implement the safe harbor principles could subject carriers to enforcement actions under the Commission's rules.

A. Notice

First and foremost, location service providers must **inform the customer** about the specific location information collection²² and use practices *before* any disclosure or use of location information takes place. There are several ways in which a service provider can inform customers about their location information practices. Notification could be included in a service agreement prior to the commencement of services. The provider could also describe location information policies in electronic mail, on a web site, or in a letter sent to subscribers. Consumers could also get notice on a bill directing subscribers to a toll-free number or Internet site address for a description of the carrier's complete policies and practices.²³

B. Consent

The hallmark of the CTIA privacy principles is the requirement for express authorization prior to any collection activity other than those specific exceptions under Sections 222(d)&(f). "Express authorization" may be made in written, oral, electronic or other form under these principles so long as it manifestly evidences the customer's desire to participate in the location service or transaction. CTIA believes that there are a myriad

²² By "collection," CTIA means the acquisition of location information other than that used to complete a call or provide a subscriber access to a network. In most wireless systems, a user's rough location (i.e., the nearest cell site) is known to the network and is an integral part of completing wireless calls. This is not a "collection" activity.

²³ Obviously, given the constraints associated with the size of the display on most wireless phones or other terminal equipment today, the notice requirement must fit the circumstances. It is not necessary, and may be impossible in any event, for the Commission to prescribe a uniform method of providing notice. Given the physical constraints, coupled with the nascent state of location-based services, a range of meaningful alternatives will better serve the public than a single, one-size-fits-all rule.

of ways that a service provider could satisfy the consent requirement, ranging from signed service agreements to web site subscriptions or “clickwrap” agreements to user signaling on a handset or PDA. The important element here is that consent be made manifest and express prior to the use of location information.²⁴

C. Security and Integrity

Location services provider should **maintain any location information collected securely**. The systems employed by the location services provider should protect the location information from both unauthorized access and disclosures to third parties. The provider should ensure that any third party to whom the location data is provided, assuming that the customer authorizes such transfers, adheres to the provider’s location information practices.²⁵

D. Technology Neutral Principles

²⁴ Consent may be express yet implicit in a transaction such as when a wireless subscriber calls a location-based concierge service seeking driving directions. Obviously, to complete the requested transaction, the concierge service must access and use the caller’s location. However, the consent, though implicit, extends only to the use of location information for that particular transaction and would not authorize any other use or disclosure without further approval by the customer. *See* Memorandum Opinion for John C. Keeney, Acting Assistant Attorney General, Criminal Division, from Richard L. Shiffrin, Deputy Assistant Attorney General, Office of Legal Counsel, U.S. Department of Justice, (Sept. 10, 1996)(filed in CC Docket 94-102)(“the caller, by dialing 911, has impliedly consented to such disclosure”).

²⁵ CTIA recognizes that fair information practices generally include an access component under this rubric. However, given that most location information is ephemeral and kept only to complete a transaction, such a requirement would not make sense. If, on the other hand, the service provider maintains location information as part of a customer profile, CTIA would support reasonable customer access to the profile to correct any inaccuracies, similar to the access provided to other call detail records.

Neither a company's privacy practices nor a consumer's privacy expectations should be determined by the nature of the location technology. Instead, location based services should be **technology neutral**. Thus, the privacy standards employed should be the same whether the service is handset or network-based.

Today, global standard bodies are in the process of defining and standardizing capabilities for determining and delivering the geographic location of wireless terminals and devices. For example, the Location Interoperability Forum is promoting a standard for location determination methods and their supporting architectures that is based on Cell-ID and Timing Advance, E-OTD (GSM), AFLT (IS-95), and MS Based Assisted GPS.²⁶ These standards efforts often include features that address privacy concerns.²⁷ CTIA supports such technology independent privacy solutions.

IV. CONCLUSION

The Commission should commence a rulemaking proceeding to address the implementation of Section 222(h) and CTIA's proposed location privacy principles. The Commission should not wait for its general CPNI rulemaking to do so. Adopting the CTIA location information principles and allowing service providers the flexibility to implement these policy prescriptions will have the dual benefit of assuring consumers

²⁶ See www.locationforum.org.

²⁷ For example, the 3GPP TS 23.271 Draft Location Services Standard currently contemplates a privacy toggle that will empower users to block transmission of location dynamically.

that location information will be guarded while new and exciting location services and applications are developed.

Respectfully submitted,

Michael Altschul
Vice President and General Counsel
Randall S. Coleman
Vice President
Regulatory Policy & Law

Albert Gidari
Of Counsel

Perkins Coie LLP
1201 Third Avenue, 48th Floor
Seattle, Washington 98101
(206) 583-8688

**Cellular Telecommunications
Industry Association**

1250 Connecticut Avenue, N.W.
Suite 800
Washington, D.C. 20036
(202) 785-0081

November 22, 2000