Before the
DEPARTMENT OF COMMERCE
Washington, D.C. 20230

In the Matter of	)	
	)	Docket No. 100402174-0175-01
Information Privacy and Innovation in the Internet	)	
Age	)	RIN 0660-XA12

COMMENTS OF CTIA – THE WIRELESS ASSOCIATION®

I. INTRODUCTION

CTIA – The Wireless Association® ("CTIA")[1] hereby submits these comments in response to the Department of Commerce Internet Policy Task Force's Notice of Inquiry seeking information on the effect of privacy law and policy on the Internet economy.[2] As CTIA's recently revised location-based services ("LBS") guidelines and best practices demonstrate, industry self-regulation is more capable of moving at Internet speeds and adapting to the ever-evolving digital world than government rulemaking and regulation in the fight to safeguard consumers' privacy. In issuing its report, CTIA urges the Department of Commerce to recognize that proactive industry self-regulation, which is responsive to consumer demands and marketplace evolution, is more nimble and effective at protecting consumer privacy in the age of the Internet than government regulation.

Few could fully anticipate a mere two decades ago the crucial role the Internet would play in the lives of Americans. In addition to the explosion of commerce and content on the Internet, Americans' increasingly are migrating to web-based services, including education,

---

[1] CTIA-The Wireless Association® (www.ctia.org) is an international organization representing the wireless communications industry. Membership in the association includes wireless carriers and their suppliers, as well as providers and manufacturers of wireless data services and products.

[2] Information Privacy and Innovation in the Internet Age, 75 Fed. Reg. 21226 (Apr. 23, 2010).

healthcare and government services. With the aggregation of personal information on the Internet, great diligence is necessary to prevent fraud and unwanted dissemination of personally identifying information ("PII"). CTIA and the wireless industry have been leaders in privacy policy, especially with respect to LBS associated with mobile users. LBS, which rely on, use or incorporate the location of a device to provide or enhance a service, have raised privacy questions from their start, more than fifteen years ago. In response, the wireless industry has crafted LBS best practices and guidelines to address consumers' concerns regarding their services. These guidelines, which CTIA recently updated to reflect changes in the technology, the market, and consumers' demands, are an example of how self-regulation has the flexibility and the speed to adapt to the rapidly evolving wireless ecosystem.

II. BACKGROUND

Even when LBS was just an idea, CTIA and the wireless industry recognized the importance of balancing the need for access to customers' location information in emergencies and legitimate law enforcement purposes with wireless users' privacy expectation. The industry's efforts to balance these expectations with consumers' demand for innovative services and devices began fifteen years ago when CTIA and Public Safety proposed a "Consensus Solution" for providing location information to Public Safety Answering Points to the Federal Communications Commission ("FCC" or "Commission") in the agency's wireless E-911 rulemaking proceeding.[3]

[3] *See* In the Matter of Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, Report and Order and Further Notice of Proposed Rulemaking, 11 FCC Rcd 18676, 18687-88, 18770 (1996) (Full text of *Consensus Agreement Between CTIA and Public Safety Groups Regarding Wireless E911* available at Appendix D, Table B).

In the late 1990s, CTIA supported *The Wireless Communications and Public Safety Act of 1999* ("WCPSA").[4] The Act addressed some of the issues that arose from the FCC's E-911 rulemaking, including a provision that specifically authorized carriers to provide call location information concerning a user of a commercial mobile service to: (1) emergency dispatchers and emergency service personnel in order to respond to the user's call; (2) the user's legal guardian or family member in an emergency situation that involves the risk of death or serious physical harm; or (3) providers of information or database management services solely for purposes of assisting in the delivery of emergency services.[5] The WCPSA also amended Section 222 of the Communications Act of 1934, as amended ("Communications Act"), to require "the express prior authorization of the customer" for the disclosure of the wireless customer's location information for any other purpose, thus keeping consumers in control and better protecting their private location information.[6]

CTIA continued its privacy efforts in 2000 by petitioning the FCC to adopt a set of Fair Location Information Practices for wireless LBS.[7] Embracing the Federal Trade Commission's ("FTC") "belief that greater protection of personal privacy . . . will benefit businesses as well as consumers by increasing consumer confidence and participation in the . . . marketplace," CTIA modeled its proposal on the familiar FTC Fair Information Practice Principles, which espoused notice, consent, security and integrity of information,

---

[4] The Wireless Communications and Public Safety Act of 1999, Public Law 106-81, 113 Stat. 1286 (codified at 47 U.S.C. § 222 (2006)).

[5] *Id*.

[6] 47 U.S.C. § 222.

[7] Wireless Telecommunications Bureau Seeks Comment On Request to Commence Rulemaking To Establish Fair Location Information Practices, *Public Notice*, 16 FCC Rcd 5599 (2001).

and technology neutral rules.[8] Although the FCC declined to adopt CTIA's proposal at the time,[9] the fundamental principles of customer "notice" and "consent" have been widely adopted in numerous cross-industry privacy policies and principles, and have provided the basis for the wireless industry's approach to protecting the privacy of wireless users who use LBS.

III. CTIA'S LBS BEST PRACTICES AND GUIDELINES ARE ADAPTING IN LIGHT OF RAPIDLY-EVOLVING TECHNOLOGY AND CONSUMER DEMAND FOR PROMOTING AND PROTECTING THE PRIVACY OF LOCATION INFORMATION.

A. CTIA's 2008 LBS Guidelines Sought and Achieved Consensus to Establish an Effective Framework and a Strong Foundation

In 2008, as the development and deployment of LBS began occurring in earnest for non-E-911 applications, CTIA commenced work with its members and other interested parties on developing a set of industry "Best Practices and Guidelines" to promote and protect the privacy of wireless customers' location information. As part of the development process, CTIA reached out to privacy experts from over 90 entities, including telecommunications companies, non-profit privacy groups and government agencies, and examined numerous privacy agreements from various LBS companies.

---

[8] *See* Federal Trade Commission *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress*, 34 (May 2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

[9] *See* In the Matter of Request by Cellular Telecommunications and Internet Association to Commence Rulemaking to Establish Fair Location Information Practices, 17 FCC Rcd 14832 (2002). In declining to commence a rulemaking to adopt rules to implement the wireless location information privacy amendments to Section 222 of the Communications Act, the Commission stated that it "[does] not wish to artificially constrain the still-developing market for location-based services," and that it will "initiate a rulemaking proceeding only when the need to do so has been clearly demonstrated." *Id*. at 14832.

After extensive work and consultation, CTIA unveiled its Best Practices and Guidelines for Location-Based Services ("2008 Guidelines") on April 2, 2008.[10]

The 2008 Guidelines, built on the now familiar foundation of "Notice-and-Consent," directed entities that provide LBS to inform consumers about how their location information will be used, disclosed, and protected so that consumers can make an informed decision about whether or not to use a particular LBS or authorize disclosure of their location to others. Importantly, the 2008 Guidelines were expansive in scope by applying to *all* LBS providers, including application developers and equipment providers, and not simply limited to wireless carriers. Once a user has opted to use an LBS, or authorized disclosure of his or her location, the 2008 Guidelines contemplated that the user should have the ability to decide when or whether location information may be disclosed to third parties, as well as providing that the user should have the ability to revoke such authorization at any time. Furthermore, the guidelines incorporated the Notice-and-Consent structure utilized by the FTC.[11] In constructing the 2008 Guidelines, CTIA also recognized that user privacy must be balanced with legitimate law enforcement and emergency or other needs – consistent with Section 222 of the Communications Act and the FCC's rules governing Customer Proprietary Network Information.[12] Accordingly, the Guidelines do not apply to location information used or disclosed: (1) as authorized or required by applicable law (*e.g.*, to respond to emergencies, E911, or legal process); (2) to protect the rights and property of LBS

[10] News Release, CTIA – The Wireless Association®, CTIA – The Wireless Association® Announces Best Practices for Location-Based Services (Apr. 2, 2008).

[11] *See* Federal Trade Commission, Fair Information Practice Principles, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited May 27, 2010).

[12] *See* 47 U.S.C. § 222.

providers, users or other providers of location information; (3) for testing or maintenance in the operation of any network or LBS; or (4) in the form of aggregate or anonymous data. With a base of broad industry support, the 2008 Guidelines presented LBS providers with a clear path forward in the development of LBS, while giving consumers the information and tools they need to control the use of their location information.

B. CTIA's LBS Best Practices and Guidelines Are Adapting to Technological and Market Changes

Reflecting the rapid innovation and introduction of new technologies that characterize the wireless industry, CTIA's LBS Best Practices and Guidelines are not carved in stone. In fact, its framers anticipated that, as technology and applications advanced, so must the Guidelines. Accordingly, a little more than a year after publication of the 2008 Guidelines, CTIA proactively initiated efforts to update the LBS Guidelines to keep pace with the rapid advance of LBS technologies and services. These efforts produced revised Guidelines that maintain the Notice-and-Consent format while adding greater protections for LBS consumers. Of particular significance to this proceeding is the wireless industry's willingness and ability to adopt and modify best practices at the pace of Moore's Law,[13] which demonstrates the superior speed and flexibility of industry self-regulation versus government intervention.

Until recently, LBS relied on a wireless carrier having access to a user's location information and then using or sharing that information with a third party to provide an LBS. This is the model Congress contemplated when it enacted the LBS amendments to Section 222 in 1999, and even the model CTIA, commenters and participating entities contemplated when drafting the 2008 Guidelines. However, in just two years the

[13] *See* Intel, *Moore's Law: Raising the Bar* (2005), *available at* http://download.intel.com/museum/Moores_Law/Printed_Materials/Moores_Law_Backgrounder.pdf

wireless industry and LBS technology have undergone profound changes that extend the provision of LBS well beyond a carrier-centric approach.

Smartphones are rapidly taking over the market - in the fourth quarter of 2009, thirty-one percent of all handsets sold were smartphones compared to just eleven percent during the first half of 2007.[14] Leading smartphone operating systems are open for application development spurred by Android, iPhone and other application development kits, which has led to an exponential rise in applications. In late 2009, a CTIA filing with the FCC observed that consumers had access to more than 100,000 apps.[15] That number has more than doubled to 240,000, and it is projected that worldwide downloads from mobile application stores will exceed 21 billion by 2013.[16]

With increased functionality of handsets and the ease of mobile application development, LBS-based applications are on the rise and can now be downloaded to a handset and operated without the wireless carrier's involvement or knowledge. LBS technology that resides in the handset, not the carrier's network, has led to applications such as Loopt, Foursquare, Yowza!!, and Gowalla, and offers consumers

---

[14] *See* Press Release, The NPD Group, The NPD Group: Smartphones Drive More Handset Sales Overall, But Lower Prices Stall Total Handset Revenue Growth (Mar. 17, 2010), *available at* http://www.npd.com/press/releases/press_100317.html; Press Release, The NPD Group, The NPD Group: Year-Over-Year U.S. Mobile Phone Sales Increased 14 Percent in Second Quarter (Aug. 15, 2007), *available at* http://www.npd.com/press/releases/press_070815.html.

[15] In the Matter of Fostering Innovation and Investment in the Wireless Communications Market, A National Broadband Plan For Our Future, GN Docket Nos. 09-157, 09-51, Comments of CTIA (Sept. 30, 2009).

[16] *Consumers Will Spend $6.2 Billion in Mobile Application Stores in 2010*, CELLULAR-NEWS (Jan. 18, 2010), http://www.cellular-news.com/story/41491.php.

location-specific driving directions, mobile search, coupons, reviews, and social networking. Loopt alone has reached over three million registered users.[17]

At the same time, the past two years have seen increased consumer consciousness and demand for privacy. From Facebook and Google, and their use of consumer data, to the forthcoming Supreme Court decision in *City of Ontario, CA v. Quon*, which examines the expectation of privacy in an employer-provided wireless device, privacy policies and frameworks are on the front pages of newspapers and web sites, and in the minds of consumers.[18]

In 2009, CTIA and its members began the process of revising the LBS Guidelines to ensure consumers that when they use an LBS, a clearly identified LBS provider will inform them about how their location information will be used and disclosed, and the LBS provider also will obtain their consent before initiating services. The revised Guidelines, released in March 2010, merge the familiar Notice-and-Consent requirements with protections for account holders and device users alike.[19]

As stated in the revised Guidelines, LBS providers will use written, electronic or oral notice that will ensure that users have an opportunity to be fully informed of the providers' information practices. Notice must be provided in plain, easily understood language; it must not be misleading and, if combined with other terms or conditions, the portion pertaining to the LBS must be conspicuous. If, after having obtained consent, an LBS provider wants to use location information for a new or materially different purpose

---

[17] Claire Cain Miller, *Cellphone in New Role: Loyalty Card*, NEW YORK TIMES (May 31, 2010), *available at* http://www.nytimes.com/2010/06/01/technology/01loopt.html (last visited June 1, 2010).

[18] Quon v. Arch Wireless Operating Co., 529 F.3d. 892 (9th Cir. 2008) *cert. granted*, 130 S.Ct. 1011 (U.S. Dec. 14, 2009) (No. 08-1332).

[19] *See* 2010 Revised Guidelines, attached hereto at Attachment A.

not disclosed in the original notice, the provider must inform the user with further notice and obtain the user's consent to the new or other use. LBS providers must inform users how long any location information will be retained, if at all. The Guidelines require that, as a general matter, providers should retain user location information only as long as business needs require, after which such information should be destroyed or rendered unusable. The Guidelines also direct LBS providers to periodically remind users when their location information may be shared with others and of the users' location privacy options. A significant change from the 2008 Guidelines is the clear requirement that every *user*, not just account holders, be informed whenever an LBS is installed and used on their device, reducing the risk of surreptitious or unauthorized tracking.

The revised Guidelines require that consent be informed and based on a notice consistent with the notice requirements set forth by the Guidelines. Consent may be implicit, such as when users request a service that obviously relies on the location of their device – such as seeking information on the nearest gas station. Notice may be contained in the terms and conditions of service for a location-based service to which users subscribe. Users may manifest consent to those terms and conditions electronically by clicking "I accept;" verbally by authorizing the disclosure to a customer service representative; through an interactive voice response system or any other system reasonably calculated to confirm consent. The Guidelines expressly reject pre-checked boxes that cause a user to be automatically opted-in to location information disclosure or choice mechanisms that are buried within a lengthy privacy policy or a uniform licensing agreement. Such an approach would be insufficient to express user consent under the CTIA Guidelines.

The revised Guidelines offer a framework for the protection of user privacy. The industry's willingness to develop meaningful and effective best practices, and to nimbly revise those guidelines as circumstances warrant, represents the best way to balance the need to promote and protect user privacy while also facilitating the deployment of new and innovative products and services. Industry self-regulatory efforts have the flexibility to address privacy issues in the ever-changing wireless space much faster than government regulation.

C. Data Retention Requirements Adversely Affect Carriers, Consumers, and the Internet Economy

Data retention requirements currently under consideration have real economic and privacy implications for providers. The "Internet Economy" – as used by NTIA in this proceeding – will be adversely affected by data retention laws that require carriers not only to store large quantities of data for law enforcement purposes, but also to implement additional costly measures in order to ensure the safety of consumers' private information. While complying with such data retention regulations, carriers are often exposed to privacy and Fourth Amendment lawsuits. The ultimate result is a stifling of innovation and investment in the Internet.

A balance between law enforcement's legitimate need to investigate and prosecute crimes carried out or facilitated by the Internet, consumers' legitimate expectations of privacy and free speech, and carriers' costs of retention and its effect on innovation and creativity on the Internet must be sought at the Federal level. As a recent NTIA report stated, "[i]f states are allowed to set their own data retention standards, this would burden the [Internet service providers] with as many as 54 different sets of

requirements, creating even more uncertainty for law enforcement."[20] Government, privacy advocates and industry must work together to develop a technologically feasible and economically reasonable solution with careful attention to constitutional and legal protections.

[20] National Telecommunications and Information Administration, Youth Safety on a Living Internet: Report of the Online Safety and Technology Working Group (June 4, 2010), *available at* http://www.ntia.doc.gov/reports/2010/OSTWG_Final_Report_060410.pdf

IV. CONCLUSION

With the emergence of new technology and applications, today's wireless ecosystem is vastly different from just a few years ago. Advances in wireless technology are being driven by Moore's Law, and when innovative new technologies and applications upset old paradigms, consumer privacy must keep pace. As CTIA and the wireless industry have shown, proactive industry self-regulation that is responsive to consumer demands and marketplace evolution will be more nimble and effective at protecting consumer privacy in the age of the Internet than government regulation.

Respectfully submitted,

By: */s/ Brian Josef*
Brian Josef
Director, Regulatory Affairs

Michael F. Altschul
Senior Vice President, General Counsel

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

CTIA–The Wireless Association®
1400 16th Street, NW, Suite 600
Washington, DC 20036
(202) 785-0081
www.ctia.org