Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

LOCATION-BASED SERVICES

AN OVERVIEW OF OPPORTUNITIES

AND OTHER CONSIDERATIONS

Wireless Telecommunications Bureau
May 2012

Table of Contents

I. EXECUTIVE SUMMARY

Technological innovations, notably over the past decade, facilitate the collection of substantial amounts of personally identifiable data about virtually anyone who accesses information online. The rapid pace of change in both technology and business models is fueling an active and growing debate in the United States and around the world about the appropriate use of that data. The following report focuses on one part of the discussion: Location-based services ("LBS"), mobile services that combine information about a user's physical location with online connectivity and are transforming the way Americans work and play.

Among other things, LBS let users access relevant and up-to-date information about their surroundings, inform others of their whereabouts, and get instant access to maps and traffic information for their current location. Whether used for fleet tracking or inventory management, for machine-to-machine communications, or for social networking or entertainment, LBS can create a more dynamic user experience that adds value and convenience and changes the way people transact business and organize their activities and free time.

Not surprisingly, Americans are quickly adopting LBS. As of May 2011, 28 percent of adult Americans used mobile LBS of some type.[1] LBS are expected to deliver $700 billion in value to consumers and business users over the next decade.[2]

The promise of LBS, however, comes with challenges and concerns. Because mobile devices have the ability—and often the technical requirement—to regularly transmit their location to a network, they also enable the creation of a precise record of a user's locations over time. This can result in the creation of a very accurate and highly personal user profile, which raises questions of how, when and by whom this information can and should be used.

---

[1] McKinsey Global Inst., *Big data: The next frontier for innovation, competition, and productivity* 85 (2011), *available at* http://www.mckinsey.com/mgi/publications/big_data/pdfs/MGI_big_data_full_report.pdf.

[2] *Id.*

In light of these developments, the staff of the Federal Communications Commission (the "FCC" or "Commission") has prepared this report on LBS. As discussed in greater detail below, drawing upon its experience in protecting consumer privacy, Commission staff believes:

- LBS have tremendous potential to provide value and foster innovation to benefit the economy and consumers;
- LBS industry players face challenges as they attempt to provide consumers with appropriate notice and choice with respect to the use of the data generated by LBS and the devices and networks that host them;
- Industry is taking steps to respond to these challenges but the degree of responsiveness varies among companies and industry segments; and
- New issues continue to emerge that need to be addressed, timely and responsively.

Consequently, in collaboration with federal partners and industry representatives, Commission staff will continue to monitor industry compliance with applicable statutory requirements and evolving industry best practices to ensure LBS evolves to meet its fullest potential while protecting the legitimate interests of consumers in safeguarding their personally identifiable information.

II. INTRODUCTION

The FCC has decades of experience protecting consumer privacy by implementing privacy protection statutes, providing technical and policy guidance on privacy issues, and interacting with other agencies and representatives of the Executive Branch to develop a consistent approach to privacy protection. As the expert agency on communications and broadband networks, the Commission has an important role in protecting consumer privacy in the future.

Consistent with this role, on June 28, 2011, the FCC hosted a full-day workshop on LBS and the privacy issues they raise.[3] Participants included privacy policy experts as well as representatives from a cross section of companies active in enabling LBS, including technology, broadband and LBS providers and entrepreneurs. The workshop sought to raise awareness about the potential of LBS while highlighting the need to protect the basic ideals of consumer choice and privacy. At the workshop the agency gathered information from wireless carriers, application developers and business and academic leaders about trends in the development and use of LBS. Among the issues explored was a review of industry best practices for protecting personal information and what consumers should know about protecting themselves while using these services. Stakeholders recognized the importance of addressing privacy questions in order to protect basic privacy values as well as making sure consumer concerns about the use of their location information and its security do not slow adoption of innovative services or opportunities.[4]

Other agencies, including the Federal Trade Commission ("FTC") and the Department of Commerce, also have been assessing mobile privacy issues, raising consumer awareness, and encouraging proactive industry involvement to address challenges and concerns. In addition, Congress conducted several hearings that addressed location data privacy.[5] These hearings have

---

[3] *See FCC Staff to Host Forum Aimed at Helping Consumers Navigate Location-Based Services*, Public Notice, 26 FCC Rcd 6757 (2011).

[4] *See* App. B (Agenda for FCC Forum); Section V, *infra* (discussing the FCC forum).

[5] *See, e.g.*, *Internet Privacy: The Views of the FTC, the FCC and NTIA: Hearing Before the Subcomm. on Commerce, Manufacturing, and Trade and the Subcomm. on Communications and Technology of the H. Committee on Energy and Commerce*, 112th Cong. (July 14, 2011), http://energycommerce.house.gov/hearings/hearingdetail.aspx?NewsID=8769; *Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Comm. on the Judiciary*, 112th Cong. (May 10, 2011), http://www.judiciary.senate.gov/hearings/hearing.cfm?id=e655f9e2809e5476862f735da16bd1e7; *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution , Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. (June 24, 2010), http://judiciary.house.gov/hearings/printers/111th/111-109_57082.PDF; *The Collection and Use of Location Information for Commercial Purposes:*

dealt generally with the rapidly changing technology, the surge in LBS and the need to ensure the protection of the privacy rights of LBS users through the development of appropriate policy frameworks. Legislation dealing with LBS privacy issues also has been introduced.[6] There have been important industry-led efforts as well.[7]

LBS offer great potential for both business and consumers. But with that potential comes the need to better inform LBS users about privacy considerations and ensure the confidentiality and protection of their personal and proprietary information. This staff report offers an overview of the opportunities and challenges of LBS. It reviews the Commission's role in protecting consumer privacy and describes the Commission's LBS Forum, which includes an explanation of the underlying technologies. It also provides a description of LBS offerings and related privacy issues, and concludes with a discussion of other government efforts with respect to LBS.

III. THE FCC'S ROLE IN PRIVACY REGULATION AND ENFORCEMENT

The Commission's involvement in the protection of consumer privacy is rooted in the Communications Act of 1934, as amended (the "Act"), which charges the FCC with implementing a number of privacy protection provisions. Section 222 of the Act and our implementing rules, for example, require telecommunications carriers and interconnected Voice over Internet Protocol ("VoIP") providers to secure customer proprietary network information ("CPNI").[8] The FCC has adopted rules implementing Section 222 of the Act to address the

---

Hearing Before the Subcomm. on Commerce, Trade and Consumer Protection and the Subcomm. on Communications, Technology, and the Internet of the H. Comm. on Energy and Commerce, 111th Cong. (Feb. 24, 2010), http://democrats.energycommerce.house.gov/index.php?q=hearing/the-collection-and-use-of-location-information-for-commercial-purposes.

[6] *See* Section VII.C., *infra*.

[7] *See* Section VI, *infra*.

[8] 47 U.S.C. § 222. CPNI includes "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by a customer of a telecommunications service, and that is made available to the carrier solely by virtue of the carrier-customer relationship" and information contained in customers' telephone bills except for subscriber list information. *Id.* § 222(h)(1).

handling, use, and sharing of CPNI, as well as rules to prevent pretexting, the practice by which unauthorized third parties attempt to gain access to telephone subscribers' CPNI.[9] Through rulemakings and enforcement actions, the FCC has resolved difficult issues related to its CPNI rules, including establishing minimum notice standards, determining when opt-in and opt-out choices for consumers are appropriate, adopting data sharing rules and reasonable data security measures, and requiring notification to law enforcement and consumers in the event of data breaches.[10] As a result of the Commission's actions, the Section 222 protections are sound, well understood by industry and consumers, and judicially approved.[11] Thus, the Commission has seen the number of consumer complaints related to CPNI decline steadily.[12]

Other sections of the Act require communications providers to protect personal information. Sections 338(i) and 631 establish requirements for satellite and cable television providers, respectively, for the treatment of their subscribers' personally identifiable information ("PII").[13] Specifically, these provisions require clear and conspicuous notice about collection and use of PII, limit disclosure of PII, and require cable and satellite providers to employ reasonable levels of security for their subscribers' PII.[14] In addition, Sections 338(i) and 631 contain private

[9] 47 C.F.R. § 64.2001 – 64.2011.

[10] *See, e.g., Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Third Report and Order and Third Notice of Proposed Rulemaking, 17 FCC Rcd 14860 (2002).

[11] *See, e.g., NCTA v. FCC*, 555 F.3d 996 (D.C. Cir. 2009).

[12] *Privacy and Data Security: Protecting Consumers in the Modern World: Hearing Before the S. Comm. on Commerce, Science, & Transportation*, 112th Cong. (June 29, 2011) (statement of Austin C. Schlick, General Counsel, Federal Communications Commission), http://commerce.senate.gov/public/?a=Files.Serve&File_id=8380ddf6-cdd7-4ca9-8f2d-ad511691b5a3.

[13] 47 U.S.C. §§ 338(i), 551. "Personally identifiable information" is not defined in the statute, but can be assumed to include "all individually identifiable information collected by a cable operator over a cable system regarding its subscribers." H.R. Rep. No. 934, 98th Cong., 2d Sess. (1984).

[14] 47 U.S.C. §§ 338(i), 551.

rights of action such that consumers have a legal remedy if their PII is improperly collected, used or disclosed.[15]

In addition to enforcing the Act's privacy provisions, the Commission has engaged in numerous initiatives to address privacy concerns. The Commission has established an internal working group comprised of experts from different bureaus and offices who meet periodically to examine privacy issues, developments in privacy laws and issues, location-based issues, and online security issues. This group also has conducted information gathering meetings on privacy issues with representatives of the cable industry, the satellite industry, telecommunications carriers, and trade associations.

Educating consumers about privacy and data security is an important priority at the Commission. The agency's Consumer and Governmental Affairs Bureau issues Consumer Alerts and makes available Factsheets addressing privacy and security issues.[16] It also devotes sections on its website to informing consumers about how to protect their privacy. In addition, the Commission's Consumer Help Center is staffed with personnel trained to answer questions from callers on several different issues including privacy concerns. The Commission created an online guide for consumers showing how to activate encryption features on wireless routers to help consumers secure their home networks and developed a Cybersecurity Tip Sheet to help small businesses understand and implement precautions to secure their networks.[17]

The Commission works collaboratively with other federal agencies, as well as consumer, educational, and other privacy groups, to educate consumers and ensure consistency across the government in protecting privacy. The FCC and the FTC have a joint task force devoted to

---

[15] *Id.* at §§ 338(i)(7), 551(f).

[16] *See* http://www.fcc.gov/encyclopedia/consumer-publications-library#Privacy.

[17] *See* FCC Consumer Tip Sheet, "Wi-Fi Networks and Consumer Privacy" (Apr. 17, 2012), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db0417/DOC-313634A1.pdf; *see also* http://www.fcc.gov/cyberforsmallbiz (setting forth practical cybersecurity tips for small businesses).

examining privacy issues generally and location-based privacy issues specifically. The Commission also has partnered with the FTC on education efforts like Net Cetera and OnGuard Online, which offer consumers advice on how to protect their children's personal information, guard against identity theft, and avoid e-mail and phishing scams. FCC staff also participated in an interagency task force assembled by the White House Office of Science and Technology Policy with the goal of developing administration policy on commercial data privacy issues. The Small Business Administration collaborated with the Commission on small business cybersecurity initiatives. The Commission also is a member of the National Initiative for Cybersecurity Education partnership led by the Department of Commerce and has partnered with the U.S. Chamber of Commerce, the National Urban League, and others to develop and distribute privacy and cybersecurity tip sheets and other educational materials.

The Commission's collaborative efforts have extended beyond education. Working in conjunction with the FTC, the FCC adopted "Do-Not-Call" regulations under Section 227 of the Act.[18] The FCC and the FTC also collaborate on implementation of the CAN-SPAM Act,[19] with the FCC adopting rules prohibiting sending unwanted commercial email messages to wireless accounts without prior permission.[20] In conjunction with the Department of Justice, the FCC enforces Section 705 of the Act, which restricts the unauthorized divulgence, publication, or use of certain communications.[21]

The Commission's role as an advocate and safeguard of consumer privacy was underscored by the Congressional testimony of Chairman Julius Genachowski and FCC General

[18] 47 U.S.C. § 227; 47 C.F.R. § 64.1200.

[19] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003), codified at 15 U.S.C. §§ 7701-7713, 18 U.S.C. § 1037 and 28 U.S.C. § 994.

[20] 47 C.F.R. § 64.3100.

[21] 47 U.S.C. § 605.

Counsel Austin Schlick regarding privacy issues at hearings during the summer of 2011.[22] In their testimony, both Chairman Genachowski and General Counsel Schlick discussed the three overarching goals of the Commission's approach to privacy: (1) ensuring that personal information is protected from misuse and mishandling; (2) requiring providers to be transparent about their practices; and (3) enabling consumer control and choice.[23] In his testimony, Chairman Genachowski stressed the importance of balancing the benefits provided by technology against the dangers and challenges that technology can bring, while looking to technology to be part of the solution.[24] He encouraged industry to use its expertise to empower consumers, provide transparency and protect data.[25]

IV. LBS OFFERINGS

Location-based services have great potential for growth. While estimates vary,[26] most research indicates that revenues are expected to triple in the next five years.[27] Although Apple's

---

[22] *Internet Privacy: The Views of the FTC, the FCC and NTIA: Hearing Before the Subcomm. on Commerce, Manufacturing, and Trade and the Subcomm. on Communications and Technology of the H. Committee on Energy and Commerce*, 112th Cong. (July 14, 2011) (statement of Julius Genachowski); *Privacy and Data Security: Protecting Consumers in the Modern World: Hearing Before the S. Comm. on Commerce, Science, & Transportation*, 112th Cong. (June 29, 2011) (statement of Austin C. Schlick).

[23] *Id.*

[24] *Internet Privacy: The Views of the FTC, the FCC and NTIA: Hearing Before the Subcomm. on Commerce, Manufacturing, and Trade and the Subcomm. on Communications and Technology of the H. Committee on Energy and Commerce*, 112th Cong. (July 14, 2011) (statement of Julius Genachowski).

[25] *Id.*

[26] Variations in estimates may result from different definitions of "location-based services."

[27] *See, e.g.*, Pyramid Research, Research Report, *Location-Based Services, Market Forecast, 2011-2015* (May 2011) (estimating $2.8 billion in revenues for location-based services in 2010, with growth projected to $10.3 billion in 2015), *available at* http://www.pyramidresearch.com/store/Report-Location-Based-Services.htm; Press Release, ABI Research, *Global Location-Based Platform and Infrastructure Revenues to Reach $1.8 Billion by 2015* (Mar. 15, 2010) (estimating revenues of $560 million in 2010 and $1.8 billion in 2015), *available at* http://www.abiresearch.com/press/3393-Global+Location-Based+Platform+and+Infrastructure+Revenues+to+Reach+%241.8+Billion+by+2015; Press Release, *Mobile Location-Based Services Market to exceed $12bn by 2014 driven by Increased Apps Store Usage, Smartphone Adoption and New Hybrid Positioning Technologies, According*

application store has only been in operation since July of 2008, it surpassed 25 billion downloads worldwide as of March 2012.[28] This growth trend extends to applications that rely on a user's location: 7,200 location-based applications were offered in February 2010, compared to 3,300 location-applications in July 2009.[29] In June 2011, Foursquare, the location-based social networking company, reported that it had exceeded ten million users who have "checked-in," posting their location to friends over 750 million times.[30]

LBS have facilitated the development of several types of services and applications:

- **Navigation and Travel –** Applications in this category allow a user to perform a search based in part on location, *i.e.*, to find the nearest hotel, ATM, bus stop, or particular restaurant.[31]
- **Tracking and Geosocial Networking –** Using applications in this category, users can share their location with friends, family, or strangers via online social networks. Included in this category are applications that recommend restaurants or other places of interest based on where a user's network of "friends" has checked-in, or that enables businesses to reward their customers for loyalty based on repeated visits or check-ins. Other applications in this category enable parents to track the location of their children, family and caregivers to monitor dementia patients, and pet owners to recover lost dogs. [32]

---

to Juniper Research (Feb. 2010), *available at* http://www.juniperresearch.com/press-releases.php?category=2&pg=4); *see also* Pew Internet & American Life Project, *28% of American adults use mobile and social location-based services* (Sept. 2011), *available at* http://www.pewinternet.org/Reports/2011/location.aspx.

[28] *See* Joanna Stern, *25 Billion Apps Downloaded From the Apple App Store*, ABC News (Mar. 5, 2012), *available at* http://abcnews.go.com/blogs/technology/2012/03/25-billion-apps-downloaded-from-the-apple-app-store/.

[29] Skyhook Wireless, *Location Aware App Report: Review of location-aware apps from the iPhone, Blackberry, and Android App Stores* (Feb. 2010).

[30] Remarks of Jon Steinback, Director of Marketing, Foursquare Labs, Inc., at FCC Forum.

[31] Examples of navigation and travel applications include WHERE, Yelp, Zagat, MapQuest 4 Mobile, Google Places, Yellow Pages Mobile, NextBus, OpenTable, and Star Walk.

[32] Examples of tracking and social location "check-in" applications include FourSquare, Loopt, Family Locator, Adient, Tagg, FindFriends, Gowalla, Facebook Places, Twitter, and Yelp.

- **Gaming and Entertainment –** These applications allow users to play games on their wireless devices with friends and family, persons in their local network, or anyone online. Some location-based games track phone movement and create real-life scavenger hunts. This category also includes photography and video applications that record the GPS location tags for photos and videos or allow users to add location information to their photos.[33]

- **Retail and Real Estate** – Retail applications enable consumers to find the nearest store, provide in-store maps, check real-time inventory data, or shop from their phone, while real estate applications show houses for sale or rent or in foreclosure in a given area.[34]

- **Advertising** – Location-based advertising allows users to receive ads relevant to their current location or based on patterns of frequently visited locations. The ads generally appear within other applications or in web browser windows.[35]

- **News and Weather** – These applications provide users with weather and news targeted to their specific location.[36] Some applications provide connection to local radio or TV providers for video or audio streaming, including access to police scanners.

- **Device Management** – LBS management applications allow users to track and control their wireless devices from other sources (like a home computer) or to control other devices from their wireless devices.[37] This may include tracking, locking, or erasing a lost phone, or locating, unlocking, and starting a vehicle.

---

[33] Examples of gaming and entertainment applications include Scrabble, Tourality, iPhone Camera, Flickr, and Geocaching.

[34] Examples of retail and real estate applications include Google Shopper, Target, Home Depot, HUD Homes, and Zillow Real Estate Search.

[35] Examples of advertising applications include WHERE Ads, SkyHook, go2 Media, and Smaato.

[36] Examples of news and weather applications include The Weather Channel, Weather HD, USA Today, NPR News, Stitcher Radio, ABC News, and Scanner911.

[37] Examples of device management applications include Find My iPhone, Lookout, OnStar MyLink, and myChevrolet.

- **Public Safety** – Some LBS applications principally serve public safety functions. In addition to the San Ramon Valley California Fire Protection District CPR application described above, Google is developing an "Amber Alert" application that would inform users in the possible vicinity of missing or abducted children.[38] Another application that has been developed by the University of Maryland enables students to alert campus security to an incident, provide its location, and stream live audio and video directly to the dispatcher.[39]

V. FCC FORUM ON LOCATION-BASED SERVICES

On June 28, 2011, the Commission, in consultation with the FTC, held a public education forum on LBS featuring representatives of telecommunications carriers, technology companies, consumer advocacy groups, and academia. The forum featured three panel discussions and several presentations on technology, applications, and policy implications of LBS. Topics included how LBS works, benefits and risks of LBS, industry and consumer best practices, and what parents should know about location tracking when their children use mobile devices.[40]

A. LBS Technologies

The forum began with a tutorial on location technology and associated data flows given by Professor Matt Blaze of the University of Pennsylvania.[41] According to Professor Blaze, there are three primary location technologies currently in use:

- *Cellular Sector/Base ID*. Cellular handsets must constantly register their presence with the nearest base station in order to establish service even when in standby mode.[42] Because the network operator has the exact location of each base station, the location of the

[38] Remarks of Alan Davidson, Director of Public Policy for the Americas, Google Inc., at FCC Forum.

[39] *See* http://www.emergencymgmt.com/safety/Smartphone-Application-V911-Maryland.html.

[40] *See* App. B.

[41] *See* Presentation of Matt Blaze, Univ. of Pennsylvania, *Technology and Privacy in Mobile Location Services*, *available at* http://transition.fcc.gov/presentations/06282011/matt-blaze.pdf.

[42] The implication of this network requirement is that consumers who believe they have disabled all location tracking on their mobile device may nevertheless still be sharing some location information necessary to provide service. *See infra* n.79.

handset can be resolved to within the coverage area. The radius covered can vary greatly, from several miles down to a city block or even an individual business or residence, depending on the cell density and network architecture. Increased resolution can be achieved by triangulating between overlapping cell sectors and is often used by providers to improve accuracy for emergency response and to monitor coverage.

- *Global Positioning System (GPS)*. A substantial majority of mobile handsets, as well as an increasing number of tablets and laptops, are equipped with GPS chips that allow the devices to calculate their own position to within ten meters or less. GPS can determine location independently of other technologies, though it is often used in conjunction with them to enable a quicker location fix or where the required line-of-sight to the sky is obscured. While the location can be calculated entirely by the device, it is generally in the form of simple coordinates (*e.g.* latitude and longitude), and most mobile applications need to transmit that data to third parties in order to obtain maps or other information based on the device's location.

- *Wi-Fi.* LBS leverage the Wi-Fi technologies in handheld devices that scan their surroundings for known or open networks. Wi-Fi LBS rely on active surveys of an area to note the unique identifier and location of each Wi-Fi base station. These may include everything from hotspots in coffee shops and hotels to residential and business networks. When a Wi-Fi enabled device accesses a location service, the browser or application may send to the service the coordinates of Wi-Fi networks it currently "sees," enabling the current location to be triangulated.

As Professor Blaze noted, the technology employed in LBS is evolving rapidly and is becoming more accurate, less expensive, and faster. In addition, the specific technology employed is generally transparent to the user. Depending on the application, once a user's location has been determined, it is generally transmitted to one or more entities, including third parties with whom the user may have no established commercial relationship. Parties to whom location data may be available include the wireless carrier to which the user subscribes, the handset manufacturer, operating system developer, application developer, location service

provider, advertiser or ad network, and others. According to Professor Blaze, slight shifts in an application's architecture that may adjust the amount or level of detail of personal information collected by the LBS can have profound privacy implications.[43]

B. Trends in Location Based Services

The first panel at the forum discussed current trends in LBS, including the types of LBS currently offered, potential new LBS offerings in development, and overall LBS usage trends. The panel also discussed the business and technological interactions between wireless carriers, operating system developers and application developers.[44]

The panelists first reviewed current trends in the LBS marketplace. They highlighted the continuing development of social networking applications that facilitate interaction among users by identifying their location to a network of friends. Examples of these applications offered by the panelists include Foursquare, a location-based social networking website for mobile devices that permits users to check-in to their location, and Facebook's Places, an application that allows users to voluntarily share their location to facilitate "serendipitous encounters" among a network of friends. Another trend in LBS applications noted by the panelists is reward-based applications, including applications for businesses to reward frequent customers for loyalty and user-directed reward applications that provide users with rewards for taking steps toward certain goals.

---

[43] For another useful overview of the technology behind LBS, see also *Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Comm. On the Judiciary*, 112th Cong. (May 10, 2011) (statement of Askan Soltani), *available at* http://www.judiciary.senate.gov/pdf/11-5-10%20Soltani%20Testimony%20-%20Revised.pdf ("Soltani Testimony").

[44] The participants on the first panel were Alan Chapell, Chairman of the Mobile Marketing Association's Privacy and Preferences Committee and Founder of Chapell & Associates, Kristi Crum, Executive Director – Consumer Solutions, Verizon Wireless, Alan Davidson, Director of Public Policy for the Americas, Google Inc., Carter Griffin, General Partner, Updata Partners, Tim Sparapani, Director of Public Policy, Facebook, Brandt Squires, Consultant, Squirebend LLC (previously Director Livingsocial, Co-founder BuyYourFriendADrink.com), and Jon Steinback, Director of Marketing, Foursquare Labs, Inc.

The panel also discussed the types of data needed to support these LBS applications. The panelists emphasized that the vast majority of LBS applications rely on personal information that is submitted voluntarily by consumers. For example, according to the panel, Google's Android operating system employs a "permission-based model," under which the operating system will notify the user at the time of installation that the particular application is attempting to access the user's location information and gives the user the option to share his information. In addition, the panel discussed uses of aggregate information that is not personally identifiable, for example, information about the number of mobile devices within a particular location at a given time.

These panelists also discussed the challenges posed by consumer privacy in LBS and what the industry is doing to meet those challenges. They focused on the importance of maintaining consumer privacy in order to increase trust between the consumer and the business. They also noted the sometimes conflicting goals of attaining full disclosure of privacy practices without unnecessarily impeding the user experience.

The panel ended with a discussion of whether there was any emerging consensus regarding privacy best practices for LBS. The panelists concurred that there is no "silver bullet" for privacy protections because of the vastly different LBS applications. However, panelists also agreed that companies will continue to compete in privacy innovation to try to win customers by providing superior privacy protections.

C. Company-Based Approaches to Protect Privacy

The second panel of the forum focused on company-based approaches to protecting privacy.[45] Panelists discussed measures the industry is taking to protect consumer privacy, establish industry best practices, and develop privacy-enhancing technologies. The panel also

[45] The participants on the second panel were Justin Brookman, Director, Project on Consumer Privacy, Center for Democracy and Technology , Maureen Cooney, Deputy Chief Privacy Officer, Director of Office of Privacy, Sprint Nextel, Lorrie Cranor, Associate Professor, Computer Science and Engineering and Public Policy, Carnegie Mellon University, Ted Morgan, Founder and CEO, Skyhook Wireless, Patti Poss, Counsel to the Director of the Bureau of Consumer Protection, Federal Trade Commission, and Scott Taylor, Chief Privacy Officer, Hewlett Packard.

discussed the ways in which companies provide information about their privacy policies to consumers, such as the use of consumer privacy notices and the type of information typically disclosed in these notices.

The panel discussed the role of government in promoting location privacy standards. Most panelists agreed that there is a role for the Federal Government to play in developing baseline standards for privacy practices and either promoting those practices or developing baseline privacy legislation that would mandate best practices. Panelists acknowledged that because of the diverse players in the LBS business environment, some type of baseline consumer privacy legislation to establish best practice guidelines may be beneficial. Such baseline standards would be helpful in promoting a consistent approach and setting consumer expectations, and should at a minimum require transparent disclosure of companies' privacy practices. The panelists also noted, however, that given the pace of technological development, baseline privacy standards—either as recommended best practices or as the basis for legislation—should focus on widely applicable principles and not be overly specific such that they would quickly become outdated. The panel encouraged expectation-setting, principles-based legislation as preferable over legislation prescribing specific mandates or rules.

In response to the discussion of the approaches that government could encourage, the panelists discussed the concept of "privacy by design," in which privacy is considered from the earliest stages of product development. Panelists agreed that government could be an effective advocate of such an approach in any recommended, non-binding best practices. However, it was noted that while it may be fairly simple for large developers to implement such practices, it may be more difficult for smaller application developers with limited resources to incorporate a "privacy by design" approach to their product development.

Panelists also discussed various industry efforts to develop a set of best practices. Panelists agreed that the guidelines developed by CTIA–The Wireless Association ("CTIA"), a trade association representing the wireless communications industry, provide a good starting

point. Those guidelines support notice and opt-in permission before allowing an application to access location data. Other organizations, such as the Future of Privacy Forum, have introduced best practice guidelines that could be broadly applied across the business environment.

Notwithstanding these industry efforts, panelists noted some deficiencies in current privacy practices for LBS. For example, privacy notices can vary from carrier to carrier, device to device and platform to platform, and some believe that more consistency with respect to privacy notices would benefit consumers by making them easier to follow and understand. In addition, there continues to be incomplete disclosure of the ways that location information is used after it is collected. While the reason some applications collect location information is intuitive to consumers, other applications collect location information for no obvious or apparent purpose. A consumer may have clear notice that an application will access and use her location information and be afforded the opportunity to opt-in to the service. However, what is done with location information after the application has it may not be at all transparent to the consumer, and the location information may be sent on to third parties without the consumer's permission. The panelists discussed some specific difficulties that are posed by the small screens and limited user interfaces on mobile devices, and discussed the struggle to find a user-friendly balance of disclosure detail and frequency.

D. Public Safety Opportunities with LBS

The forum then featured a presentation and demonstration of a smartphone application developed by the San Ramon Valley California Fire Protection District that can alert users trained in CPR when someone nearby is in need of assistance.[46] Fire Chief Richard Price discussed the development process and how the application uses a registered user's location in conjunction with existing public safety systems to greatly increase the likelihood that someone in distress will receive life-saving assistance within the critical first ten minutes of the onset of cardiac distress. He also discussed some of the non-technical issues considered in the development of the

[46] http://firedepartment.mobi.

application, such as the applicability of Good Samaritan laws to users of the application and concerns around retention of the location data.

E. Consumer Education in LBS

The final panel of the forum focused on the importance of educating consumers about how to protect their personal information while utilizing LBS.[47] The panel focused in particular on the challenges of protecting children in this environment and the importance of providing information to parents about location tracking when their children use mobile devices.

The panelists discussed the importance of consumer education in this area. Both industry and company representatives on the panel agreed that consumer education efforts play a vital role in the development and expansion of LBS. In particular, panelists noted that the "privacy by design" concept of product development discussed during a prior panel contemplated education and outreach at the earliest stages of location-based product development to maximize the opportunities to increase awareness of privacy issues.[48]

The panelists also discussed the importance of educating parents and providing them with the tools to protect their children while using LBS. The panelists stressed that encouraging parents to make informed choices about sharing information requires the provision of understandable, accessible information about the implications of those choices. The panelists agreed that education efforts should focus on finding the balance between reaping the benefits of LBS while remaining aware of the potential pitfalls of such applications. This may be particularly challenging for younger generations who, panelists noted, tend to be less concerned about privacy than their parents.

---

[47] The participants on the final panel were Michael Altschul, General Counsel, CTIA-The Wireless Association, Edward G. Amoroso, Senior Vice President and Chief Security Officer, AT&T Services, Inc., Stephen Balkam, CEO, Family Online Safety Institute, Brendon Lynch, Chief Privacy Officer, Microsoft, Alan Simpson, Vice President of Policy, Common Sense Media, and Nat Wood, Assistant Director, Division of Consumer and Business Education, Bureau of Consumer Protection, Federal Trade Commission.

[48] *See supra* at 15.

The panel also discussed concerns about using LBS to market to children. Some panelists noted that marketing and advertising directly to children is among the concerns about LBS frequently mentioned by parents due to the potential to have an undue influence over children. In addition, the undesirability of such marketing and advertising made lead people to refrain from adopting and thereby benefiting from LBS. Existing laws, such as the Children's Online Privacy Protection Act ("COPPA"), attempt to regulate the marketing and advertising directed at children, and many of the government and industry education efforts, such as OnGuardOnline.gov, are directed toward teaching parents and children how to minimize receipt of location-based advertising and marketing.

The forum concluded with remarks from Peter Swire, Professor of Law at Ohio State University and former Chief Counselor for Privacy in the Office of Management and Budget during the Clinton Administration.[49] He summarized the forum by describing the tremendous potential of LBS and all the benefits that can flow from those services, while also highlighting the potential risks to consumers. Professor Swire noted that notice and choice are central to the policy discussion and consumers must be given sufficient information to make informed choices even on mobile devices with their interface limitations. Given the rapid change in the technology and marketplace, he proposed the "best practices" approach as the most effective and the most likely to lead to widespread compliance among the major players. He also noted that the role for government should be to encourage these practices and greater transparency. He reiterated that good privacy policies must address data retention and security.

VI. PRIVACY ISSUES FOR LBS

As discussed above, LBS hold great potential for spurring economic development and job creation. However, as the industry continues to develop, companies remain mindful of the associated privacy challenges. A 2009 survey of LBS users conducted by Carnegie Mellon

[49] *See* Presentation of Peter Swire, Ohio State Univ., *Wrap Up on Privacy and Location Based Services*, *available at* http://apps.fcc.gov/ecfs/document/view?id=7021690869.

University found that in general, consumers believe that the privacy risks of sharing their location outweigh the potential benefits of the services.[50] Thus, to facilitate increased adoption of these services and their attendant economic benefits, companies must address the key privacy issues associated with LBS.

A. Notice and Transparency

One of the most important aspects of companies' approaches to privacy is that they provide transparent notice to consumers regarding the company's privacy practices, informing the consumer as to what the company is doing with the personal information it collects. Such notice to consumers should be clear, concise, and an accurate reflection of the privacy practices of the company. Common elements of privacy notices to consumers include: categories of personal information collected and how that information will be used; opportunities and mechanisms for consumers to make choices regarding these uses, including opt-in or opt-out mechanisms for effectuating their choices; third-party access and sharing of personal information; and data minimization and data security practices. Some privacy notices also include information about a company's data retention policies for personal information and internal contact information to report concerns or problems with privacy.

Notice and transparency have long been recognized as core privacy principles. In the early stages of implementing Section 222 of the Act, the Commission recognized the importance of ensuring that customers receive "explicit notice of their CPNI rights" in order to facilitate informed decisions about carriers' use of that information.[51] The FTC has stressed greater transparency in privacy practices, calling for privacy notices to be "clearer, shorter, and more

---

[50] *See* Janice Y. Tsai, Patrick Gage Kelley, Lorrie Faith Cranor, Norman Sadeh, "Location-Sharing Technologies: Privacy Risks and Controls," Carnegie Mellon University at 17 (Feb. 2010).

[51] *See Implementation of the Telecommunications Act of 1996*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061 (2002).

standardized" across companies.[52] The Department of Homeland Security identified transparency as its first Fair Information Privacy Principle, recognizing the importance of "transparen[cy] and provid[ing] notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII)."[53] The Department of Commerce also recognized the value of enhanced transparency "[a]t times and in places that are most useful to enabling consumers to gain a meaningful understanding of privacy risks…."[54]

In the context of LBS, providing accurate notice and transparency of privacy practices to customers remains an important challenge.[55] As discussed at the FCC Forum, there is "limited real estate" on mobile phones, and thus they are not receptive to long, involved privacy notices.[56] A recent survey of 89 location-based applications conducted in connection with a Carnegie-Mellon study found that only 66 percent of those applications had privacy policies in place to inform users as to how personal information was treated.[57] Similarly, the Future of Privacy Forum examined the top 30 paid mobile applications across the leading operating systems as of

---

[52] "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policy Makers," FTC Privacy Report at 60 (Mar. 2012), *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf ("FTC Privacy Report").

[53] *See* "Privacy Policy Guidance Memorandum," Dept. of Homeland Security, Memorandum No. 2008-01 at 3 (Dec. 29, 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[54] "Commercial Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy," Dept. of Commerce Internet Policy Task Force at 14 (Feb. 2012) *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf ("Privacy Blueprint").

[55] Ginger Myles, Adrian Friday and Nigel Davies, "Preserving Privacy in Environments with Location-Based Applications," Pervasive Computing, IEEE Computing Society at 56 (January-March 2003) ("An important first step in protecting users' location privacy is notifying them of requests for this information.").

[56] Remarks of Peter Swire, C. William O'Neill Professor of Law, Moritz College of Law of the Ohio State University, at FCC Forum. A recent FTC workshop on mobile payments featured a session addressing the unique challenges of privacy notices on mobile devices. *See* "Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments" (Apr. 26, 2012), *available at* http://www.ftc.gov/bcp/workshops/mobilepayments/.

[57] *See supra* n.50 at 8.

May 2011 and found that 22 of those "lacked even a basic privacy policy."[58] In December 2010, the *Wall Street Journal* found that 45 of the 101 smart phone applications it examined did not have privacy policies to inform users of what personal information the application was collecting and using.[59]

Organizations continue to look for ways to make transparency of privacy practices for LBS consistent across services and easy for consumers to understand. Several industry associations have adopted best practices for privacy policies, including guidance on the provision of notice. CTIA highlights the importance of notice in its 2010 Best Practices and Guidelines for Location-Based Services:

> An important element of the Guidelines is notice. LBS Providers must ensure that potential users are informed about how their location information will be used, disclosed and protected so that they can make informed decisions whether or not to use the LBS, giving the user ultimate control over their location information.
>
> The Guidelines do not dictate the form, placement, terminology used or manner of delivery of notices. LBS Providers may use written, electronic or oral notice so long as users have an opportunity to be fully informed of LBS Providers' information practices. Any notice must be provided in plain language and be understandable. It must not be misleading, and if combined with other terms or conditions, the LBS portion must be conspicuous.[60]

The Mobile Marketing Association (MMA), a trade association representing the interests of companies in the mobile marketing value chain, also highlights the importance of accurate and transparent consumer notice in its Mobile Location Based Services Marketing Whitepaper:

> Notification: It is appropriate to notify the end-user about how their location information will be used, disclosed and protected so that a potential LBS user can make an informed decision whether or not to use the service or authorize the

---

[58] http://www.futureofprivacy.org/2011/05/12/fpf-finds-nearly-three-quarters-of-most-downloaded-mobile-apps-lack-a-privacy-policy/.

[59] Scott Thurm and Yukari Iwatani Kane, "Your Apps Are Watching You," *Wall Street Journal* (Dec. 17, 2010), *available at* http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.

[60] Best Practices and Guidelines for Location-Based Services, CTIA-The Wireless Association, at 3 (Mar. 23, 2010), *available at* http://www.ctia.org/business_resources/wic/index.cfm/AID/11300 ("CTIA Best Practices").

> disclosure. This notice should be optimized for display within a mobile device so it is easy for end-users to navigate and read.[61]

The Direct Marketing Association (DMA), a trade association supporting multichannel direct marketing tools and techniques, highlights the importance of notice and transparency in its standards for location-based marketing in its Guidelines for Ethical Business Practice:

> [M]arketers should inform individuals how location information will be used, disclosed and protected so that the individual may make an informed decision about whether or not to use the service or consent to the receipt of such communications. Location-based information must not be shared with third-party marketers unless the individual has given prior express consent for the disclosure.[62]

Individual companies have recognized the importance of notice and transparency in connection with their provision of LBS. According to Microsoft:

> When the user makes a decision to allow an application to access and use location data, Microsoft provides a link to the Windows Phone Privacy Statement, which includes its own section on location services with information describing the data Windows Phone 7 collects or stores to determine location, how that data is used, and how consumers can enable or disable location-based features.[63]

Verizon Wireless notes that it "clearly discloses how it uses and collects location information in its online privacy policy and within these applications themselves."[64] Foursquare recognizes the importance of providing "transparency of our privacy practices" to users of its location-based service.[65] Several companies have separate sections of their privacy policies specifically devoted

---

[61] Mobile Location Based Services Marketing Whitepaper, Mobile Marketing Association, at 17 (Oct. 2011), *available at* http://www.mmaglobal.com/MobileLBSWhitepaper.pdf ("MMA White Paper").

[62] Guidelines for Ethical Business Practices, Direct Marketing Association, at 42 (May 2011), *available at* http://www.dmaresponsibility.org/Guidelines/ ("DMA Guidelines").

[63] *See* Letter from Andy Lees, President, Microsoft Mobile Communications Business, to The Honorable Fred Upton, U.S. House of Representatives (May 9, 2011).

[64] Comments of Verizon Wireless, WT Docket No. 11-84, at 2 (July 8, 2011).

[65] *See* Foursquare Labs, Inc. Privacy Policy (Jan. 12, 2011), *available at* https://foursquare.com/legal/privacy.

to providing transparency regarding personal information collected in connection with LBS.[66] AT&T also has recognized the importance of providing specific notice about location-based services, and amended its privacy policy in November 2010 to expand the information provided about those services.[67]

Transparency in privacy practices also has become a source of competition.[68] Companies that are able to demonstrate to consumers clear and consistent transparency in collection and use of personal information can be more competitive and, consequently, more profitable. The trust that is built between companies and their customers around transparency in privacy has become an essential precondition for building and maintaining productive customer relationships.[69]

B. Meaningful Consumer Choice

In addition to ensuring that consumers receive adequate notice of privacy practices, companies also face the challenge of ensuring consumers are afforded the opportunity to exercise meaningful choice with respect to the collection and use of their personal information. The concept of "choice" in privacy policies refers to providing the consumer with the opportunity to tell a company what it can and cannot do with their personal information. Choice can take the form of "opt-out," where the default option permits the company to use personal information in a particular way unless the consumer objects, or "opt-in," where the company cannot use personal information without the advance consent of the consumer.

---

[66] *See, e.g.,* Apple Inc. Privacy Policy (Oct. 21, 2011), *available at* http://www.apple.com/privacy/; Loopt, Inc. Privacy Notice (Oct. 15, 2009), *available at* https://app.loopt.com/loopt/privacyNotice.aspx.

[67] *See* Comments of AT&T Inc., WT Docket No. 11-84, at 5 (July 8, 2011).

[68] *See* Privacy Blueprint at 14 (promoting greater consistency among privacy notices to make companies' privacy practices "a more salient point of competition among different products and services").

[69] Remarks of Brendon Lynch, Chief Privacy Officer, Microsoft Corp., at FCC Forum (identifying privacy as "core to creating trust with our customer and core to our business success").

In the LBS business environment, companies encounter unique challenges to ensuring that consumers have the opportunity to make meaningful choices. One issue these companies face is whether consumer choice should be opt-out or opt-in for location information, although there appears to be a developing consensus in the LBS industry that opt-in is appropriate for such sensitive information.[70] A Zogby International Survey commissioned by Common Sense Media and conducted in August 2010 found that "the vast majority of respondents say that search engines and online social networking sites should not be able to share their physical location with other companies before they have given specific authorization."[71]

Another particular challenge facing companies is minimizing interference with the user experience while concurrently offering meaningful choice to consumers. As noted at the FCC Forum, there is a "tension between granularity and simplicity"[72]—between the desire to ensure that consumers are provided the opportunity to make meaningful choices in real time regarding the use of their location-based information and the desire to ensure a seamless user experience.[73] Companies and third party intermediaries are developing creative choice mechanisms with this in

[70] Remarks of Peter Swire, C. William O'Neill Professor of Law, Moritz College of Law of the Ohio State University, at FCC Forum ("there is a broad sense that opt in is the way to go"); *see also* Comments of the Center for Democracy and Technology, WT Docket No. 11-84 (July 8, 2011) (calling on the FCC to confirm that "in most cases, precise geolocation data should only be collected and/or shared with the informed, affirmative consent of the person whose information is being collected and/or shared"); DMA Guidelines at 41 ("Marketers should obtain prior express consent from existing and prospective customers before sending mobile marketing to a wireless device."); FTC Privacy Report at 58-59. *But see* Letter from Peter Davidson, Senior Vice President, Federal Government Relations, Verizon, to The Honorable Joe Barton, U.S. House of Representatives, at 4 (Oct. 17, 2011) (discussing use of an opt-out mechanism for new location-based targeted marketing service).

[71] *See* Memorandum from Zogby International to Common Sense Media (Aug. 24, 2010), *available at* http://www.privacylives.com/wp-content/uploads/2010/10/Final-CSM-adults-topline-8-24-10-Updated-EMBARGO.pdf; *see also* Remarks of Carter Griffin, General Partner, Updata Partners, at FCC Forum (noting that consumers want to have "very tight control over publishing location" information).

[72] Remarks of Tim Sparapani, Director of Public Policy, Facebook, at FCC Forum.

[73] *See* Ginger Myles, Adrian Friday and Nigel Davies, "Preserving Privacy in Environments with Location-Based Applications," Pervasive Computing, IEEE Computing Society, at 56 (Jan.-Mar. 2003) (noting the conflicting requirements of "the need for users to control their location privacy and the need to minimize the demands made of users").

mind, including utilizing uniform language that would allow consumers to make their privacy preferences known by categories or characteristics.

The timing of presenting consumers with options is a continuing issue for debate. Some organizations and entities support the concept of "just in time" choices in connection with LBS services in which the consumer is presented with a choice at the point of data collection.[74] In addition, there is some debate regarding how often an existing choice should be presented to the consumer for reconfirmation of the approved uses of location data, or whether a choice should be honored until the user affirmatively presents a different one.[75]

The wireless industry has acknowledged the importance of ensuring that consumers are afforded the opportunity to make meaningful choices regarding the collection and use of their personal information, particularly in connection with LBS. CTIA's Best Practices recognize this issue:

> LBS Providers must obtain user consent to the use or disclosure of location information before initiating an LBS (except in the circumstances described below where consent is obtained from account holders and users are informed of such use or disclosure). The form of consent may vary with the type of service or other circumstances, but LBS Providers bear the burden of establishing that consent to the use or disclosure of location information has been obtained before initiating an LBS.[76]

In addition, CTIA's Best Practices recognize that consumers should be afforded the opportunity to make choices regarding the use of their personal information whenever a company proposes a new use of that information:

> If, after having obtained consent, LBS Providers want to use location information for a new or materially different purpose not disclosed in the original notice, they

---

[74] *See, e.g.,* TRUSTe Privacy Program Requirements, *available at* http://www.truste.com/privacy-program-requirements/program-requirements.

[75] *See, e.g.,* Remarks of Peter Swire, C. William O'Neill Professor of Law, Moritz College of Law of the Ohio State University, at FCC Forum (discussing the "random act of kindness" that suggests presenting individuals with the opportunity to review their choices on a periodic basis).

[76] CTIA Best Practices at 5.

> must provide users with further notice and obtain consent to the new or other use.[77]

Similarly, the MMA has recognized the importance of consumer choice in facilitating the continued growth of mobile marketing:

> To allow continued growth, awareness and trust of mobile Location Based Marketing, it is important that marketers exercise great care to give consumers explicit and simple control of if, when, and how their location data will be used.[78]

Individually, companies have taken a variety of approaches to consumer choice. Apple acknowledges the importance of "provid[ing] its customers with the ability to control the location-based services capabilities of their devices."[79] As Microsoft has stated:

> Microsoft does not collect information to determine the approximate location of a device unless a user has expressly allowed an application to collect location information. Users that have allowed an application to access location data always have the option to access the location at an application level or they can disable location collection altogether for all applications by disabling the location service feature on their phone.[80]

Google states that "[o]pt-in consent and clear notice are required for collection and use of location information on Android."[81]

Meaningful and understandable consumer choice is a particular issue with regard to children and their use of mobile technology. One of the most promising benefits of LBS is the ability of parents with minor children to monitor the movement of one's children,[82] but attendant to that benefit is the possibility that others may be able to exploit location-based information of children. Ensuring that children and their parents understand the choices they are making

---

[77] *Id.* at 3.

[78] MMA White Paper at 4.

[79] *See* Letter from Bruce Sewell, Apple General Counsel and Senior Vice President, Legal and Government Affairs, to The Honorable Edward J. Markey, U.S. House of Representatives (July 12, 2010). *But see* Soltani Testimony, *supra* n.43, at 5-7 (discussing continued tracking and reporting of location data even though LBS on the device have been disabled).

[80] *See* Letter from Andy Lees, President, Microsoft Mobile Communications Business, to The Honorable Fred Upton, U.S. House of Representatives (May 9, 2011).

[81] Google Inc. *ex parte*, WT Docket No. 11-84 (July 8, 2011).

[82] *See supra* n.50 at 15.

regarding children's location information, as well as all of the potential ramifications of such choices, is a critical ongoing challenge facing the LBS industry.

C. Third Party Access to Personal Information

The issue of third party access to personal information has long been at the center of the privacy debate. Third party access involves the question of what entities, other than the company to which a consumer's personal information was disclosed, have access to it. This issue is inextricably tied to the transparency and choice concepts discussed above, as an important part of companies' privacy policies involves providing notice of the third parties to whom personal information is disclosed. Frequently, consumer choice mechanisms involve informing companies of the consumer's preferences for disclosure of her personal information to third parties.

Location-based services have particular challenges regarding third party access to personal information. There are many players in the LBS business environment—including, but not limited to, the wireless carrier, the operating system, and the application developer—who may have access to consumers' personal information. As noted at the FCC Forum, while LBS initially developed as carrier-centric services, device manufacturers and application developers have been central to their evolution.[83] This development has been particularly challenging for privacy issues because while wireless carriers have been addressing privacy issues for many years, in many cases application developers have not faced these issues nor do they necessarily have a staff to provide advice and counsel on these issues.[84] Furthermore, "[o]nce an app[lication] has access to

[83] Remarks of Michael Altschul, General Counsel, CTIA, at FCC Forum; *see also* Comments of AT&T Inc., WT Docket No. 11-84, at 3 (July 8, 2011) ("Third-party applications and services often determine user location without any involvement by wireless carriers.").

[84] *But see* Remarks of Peter Swire, C. William O'Neill Professor of Law, Moritz College of Law of the Ohio State University, at FCC Forum (noting that application developers that fall into this category remain minor players in this industry at this time, and that the larger players with large databases of sensitive personal information, including location information, have compliance staffs and familiarity with privacy issues).

a user's data, there are usually no rules governing its disclosure, and no controls available to consumers to regain control of it."[85]

Industry groups and associations are taking steps to encourage application developers to include basic privacy protections in the development of their product. The Future of Privacy Forum, a think tank that seeks to advance responsible data practices, provides privacy resources for mobile application providers at a dedicated website, including "recommended practices developers should adopt to best protect the privacy and security of their consumers."[86] Similarly, TRUSTe, an independent provider of online privacy solutions, has announced the availability of a free sample mobile privacy policy for mobile application developers and publishers in order to encourage these entities to integrate privacy into the development of their product.[87] The GSM Association, an international organization representing the interests of approximately 800 mobile operators worldwide, also has developed a set of privacy design guidelines for mobile application developers.[88]

Companies in the LBS business environment acknowledge the privacy challenges posed by third party access to information and have addressed it in different ways. Apple's iPhone "presents users with a prompt before any application may begin collection of geolocation information."[89] According to Microsoft, with respect to phones using the Windows operating

---

[85] Comments of the Center for Democracy and Technology, WT Docket No. 11-84 (July 8, 2011).

[86] Future of Privacy Forum Application Developer Responsible Data Use Project, *available at* http://www.applicationprivacy.org/. *See also* Remarks of Michael Altschul, General Counsel, CTIA, at FCC Forum (discussing the development of a web interface for use by application developers to identify privacy issues).

[87] *See* Press Release, "TRUSTe Extends Leadership Role in Mobile Privacy With Introduction of Free Privacy Policies for Mobile Applications" (Nov. 2, 2011), *available at* http://www.truste.com/about_TRUSTe/press-room/news_truste_free_privacy_policies_for_mobile_applications.

[88] Privacy Design Guidelines for Mobile Application Development, GSM Association (Feb. 2012), *available at* http://www.gsma.com/documents/privacy-design-guidelines-for-mobile-application-development/20008.

[89] Comments of The NetChoice Coalition, WT Docket No. 11-84, at 2 (July 8, 2011).

system, "[t]he location data stored on the phone is only accessed and used by Microsoft to calculate the location of a phone and provide it to user-authorized applications requesting location. The information stored on the phone is not made available to applications, other features of the phone or to third parties."[90] Google described its approach toward third party access to location information on its Android operating system:

> Google does not decide which applications can access location or other user information from the device. Instead, the Android operating system uses a permissions model in which the user is automatically informed of certain types of information an application will be able to access. The user may choose to trust the application by completing the installation or the user may choose to cancel the installation. An application can only access the device's GPS location or the device's network location if it displays a notice for this permission to the user at time of installation.[91]

Companies are also taking steps to ensure that third parties with whom they are affiliated are addressing privacy issues. For example, AT&T requires third party application developers that sell their applications through AT&T to have a privacy policy and to comply with the both CTIA and AT&T guidelines for LBS privacy.[92] TechAmerica notes that many companies "require or encourage third party application developers to adhere to certain privacy guidelines in order to ensure consumers' privacy is protected."[93] Microsoft has developed guidelines for application developers to build privacy and data security protections into their products.[94] However, there are limitations on companies' ability to control the privacy practices of third parties, as noted by Verizon Wireless:

---

[90] *See* Letter from Andy Lees, President, Microsoft Mobile Communications Business, to The Honorable Fred Upton, U.S. House of Representatives (May 9, 2011).

[91] *See Consumer Privacy and Protection in the Mobile Marketplace: Hearing Before the Subcomm. on Consumer Protection, Product Safety, and Insurance of the S. Comm. on Commerce, Science and Transportation*, 112th Cong. (May 19, 2011) (statement of Alan Davidson, Director of Public Policy for the Americas, Google Inc., at 6-7).

[92] Comments of AT&T Inc., WT Docket No. 11-84, at 5 (July 8, 2011).

[93] Comments of TechAmerica, WT Docket No. 11-84, at 4 (July 8, 2011).

[94] *See* Steve Lipner, Michael Howard, "The Trustworthy Computing Security Development Lifecycle," Microsoft Corporation (March 2005), *available at* http://msdn.microsoft.com/en-us/library/ms995349.

> To the extent feasible, Verizon Wireless requires that its device suppliers incorporate privacy protections that give customers some control over the collection, use and sharing of location information by these third parties through features and tools available in the device's location settings menu. Since customers can download third party applications that do not have privacy protections, however, Verizon Wireless also warns customers to use discretion when using such applications.[95]

D. Data Security and Minimization

Data security is fundamental aspect of any organization's privacy architecture. Data security refers to the technical, physical, and administrative safeguards that have been put in place to protect personal information primarily from the risks of unauthorized disclosure or access.[96] Historically, the security measures that have been expected of companies are proportional to the sensitivity of the data requiring protection. Thus, because location data is considered by consumers and industry to be particularly sensitive personal information, heightened security requirements reasonably can be expected of providers of LBS.

A related concept to data security is that of data minimization. Data minimization refers to the idea that a company will only retain personal information it actually needs and only for the amount of time that it is needed. Security vulnerabilities thus are minimized because even in the event of a security breach, the amount of data at risk has been minimized.[97] At the same time, location information can be very valuable for law enforcement investigations, which suggests a countervailing interest in retention of more information for longer periods of time.[98]

---

[95] Comments of Verizon Wireless, WT Docket No. 11-84, at n.5 (July 8, 2011).

[96] *See also* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Article 17, para. 1 (data security refers broadly to the protection of personal data "against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing").

[97] Remarks of Peter Swire, C. William O'Neill Professor of Law, Moritz College of Law of the Ohio State University, at FCC Forum ("the privacy risk can be reduced a lot if there is a limit on the time that location is kept in identifiable form").

[98] *See, e.g., ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights and Civil Liberties of the H.*

Industry groups have recognized the importance of security measures for individuals' location information. CTIA's Best Practices recommend specific safeguards for industry participants:

> LBS Providers must employ reasonable administrative, physical and/or technical safeguards to protect a user's location information from unauthorized access, alteration, destruction, use or disclosure. LBS Providers should use contractual measures when appropriate to protect the security, integrity and privacy of user location information.[99]

CTIA's Best Practices also recognize the need to limit retention and storage of location information to only what is needed:

> LBS Providers should retain user location information only as long as business needs require, and then must destroy or render unreadable such information on disposal. If it is necessary to retain location information for long-term use, where feasible, LBS Providers should convert location information to aggregate or anonymized data.[100]

Similarly, the MMA recognizes the importance of data security and data minimization:

> Security: Reasonable security measures should be used to ensure that a user's information is secure and not shared with non-affiliated third-parties. The need for effective security measures is heightened with respect to products and services targeted to children.
>
> Data Retention: It is appropriate to limit the data retention of consumer data to as long as that data is commercially useful ensuring privacy and security.[101]

Individual companies also have recognized the importance of security issues in location-based services, while at the same time ensuring that consumers take responsibility for security matters that they can control and understand that no information security system is infallible. For example, Gowalla's privacy policy specifies:

> Gowalla uses commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of your personal information. We cannot, however, ensure or warrant the security of any information you

---

Comm. on the Judiciary, 111th Cong. (June 24, 2010) (written testimony of Richard Littlehale, Assistant Special Agent in Charge, Technical Services Unit, Tennessee Bureau of Investigation).

[99] CTIA Best Practices at 7.

[100] *Id.*

[101] MMA White Paper at 17.

> transmit to Gowalla and you do so at your own risk. Once we receive your transmission of information, Gowalla makes commercially reasonable efforts to ensure the security of our systems. However, please note that this is not a guarantee that such information may not be accessed, disclosed, altered, or destroyed by breach of any of our physical, technical, or managerial safeguards.
>
> To protect your privacy and security, we take reasonable steps (such as requesting a unique password) to verify your identity before granting you access to your account. You are responsible for maintaining the secrecy of your unique password and account information, and for controlling access to your email communications from Gowalla, at all times.[102]

Loopt takes a similar approach to data security in its privacy policy:

> Loopt uses commercially reasonable physical, managerial, and technical safeguards. We cannot, however, ensure or warrant the security of any information that Loopt receives on your behalf to operate the Loopt Services or that you transmit to Loopt and you do so at your own risk. We also cannot guarantee that such information may not be accessed, disclosed, altered, or destroyed by breach of any of our physical, technical, or managerial safeguards.[103]

VII. RECENT GOVERNMENT INITIATIVES

A. Federal Trade Commission

In March 2012, the FTC released its Privacy Report.[104] This report, adopted after extensive public comment, recommends adoption of a privacy framework applicable to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device, with the exception of entities that collect only non-sensitive data from fewer than 5,000 consumers per year and do not share the data with third parties.

The privacy framework is focused around three principles. First, the FTC encourages companies to adopt a "privacy by design" approach by building privacy protections into their everyday business practices. The FTC report also urges companies to implement privacy practices throughout their organizations, such as by assigning personnel to oversee privacy issues,

---

[102] Privacy Policy of Gowalla, Inc., *available at* http://gowalla.com/privacy.

[103] Privacy Notice of Loopt, Inc. (Oct. 15, 2009), *available at* https://app.loopt.com/loopt/privacyNotice.aspx.

[104] *See supra* n.52.

training employees on privacy issues, and conducting privacy reviews when developing new products and services.

Second, the privacy framework advocates the principle of simplified consumer choice. Under the FTC's approach, consumer choice would not be necessary before collecting and using consumer data for practices that are consistent with the context of the transaction or a company's relationship with the consumer (e.g., product fulfillment, fraud prevention, internal operations, legal compliance), or are required or specifically authorized by law. For other data practices, consumers should be offered a choice at a time and in a context in which the consumer is making a decision about his or her data. Opt-in consent should be required before a company uses personal data in a manner materially different from that disclosed at the time of collection and for the collection of sensitive data, including location data, for certain purposes.

Third, the privacy framework recommends that companies take measures to make their data practices more transparent to consumers and provide consumers with reasonable access to the data that companies maintain about them. The FTC recommends that companies adopt clearer, shorter, and more standardized privacy notices to enable better comprehension and comparison of privacy practices. In addition, the FTC suggests that companies provide reasonable access to consumer data it maintains proportional to the sensitivity and intended use of the data. The report also recommended that stakeholders engage in outreach to educate consumers about the choices available to them.

The FTC report also contains a recommendation that stakeholders implement a universal mechanism to allow users to opt-out of online behavioral tracking. Such tracking involves developing profiles based on a user's web searches and online activity for the purpose of delivering personalized advertisements. The report endorsed the opt-out regime commonly known as "Do-Not-Track," which would give users more direct control over what data is collected about them.

In addition to its Privacy Report, the FTC has taken several recent actions specifically to address mobile privacy issues. The FTC has applied COPPA, which prohibits the collection of data from children under the age of 13 without express verifiable consent from a parent,[105] in an enforcement action against a mobile application developer for collecting and disclosing children's personal information without parental consent.[106] In February 2012, the FTC issued a report examining privacy disclosures in mobile applications targeted toward children.[107] Also in February 2012, the FTC issued warnings to marketers of six mobile applications that provide background screening applications that they may be in danger of violating the Fair Credit Reporting Act.[108] In April 2012, the FTC hosted a workshop to address issues arising in the mobile payments industry, including privacy issues.[109]

B. Department of Commerce

In February 2012, the Privacy Blueprint was published, summarizing the Administration's position on the protection of online consumer privacy and providing recommendations in several areas.[110] At the center of the Privacy Blueprint is a recommendation for the development of a Consumer Privacy Bill of Rights, implemented through private, industry-specific codes of conduct and legislation, which would set forth a baseline for consumer protection. The Consumer Privacy Bill of Rights would be formulated around seven principles: (1) individual control over what personal data companies collect and how they use it; (2)

---

[105] 15 U.S.C. §§ 6501–6506. The FTC has proposed revisions to its rules implementing COPPA, including clarifying that COPPA applies to mobile devices. *See* 76 Fed. Reg. 59804 (Sept. 27, 2011).

[106] *See U.S. v. W3 Innovations, LLC*, FTC File No. 102 3251, Case No. CV-11-03958-PSG (N.D. Ca. filed Sept. 8, 2011), *available at* http://www.ftc.gov/opa/2011/08/w3mobileapps.shtm.

[107] *See Mobile Apps for Kids: Current Privacy Disclosures are Disappointing*, FTC Staff Report (Feb. 2012), *available at* http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.

[108] *See* Press Release, *FTC Warns Marketers That Mobile Apps May Violate Fair Credit Reporting Act* (Feb.7, 2012), *available at* http://ftc.gov/opa/2012/02/mobileapps.shtm.

[109] *See supra* n.56.

[110] *See supra* n.54.

transparency about a company's privacy and security practices, including easily understandable and accessible, plain language statements about data practices; (3) respect for context, such that data practices are consistent with the context in which consumers provided the data, with more prominent notices for practices that are not inherent in the company/customer relationship; (4) security precautions and responsible handling of personal data; (5) consumers' right to access and correct personal data held about them commensurate with the scale, scope and sensitivity of the data; (6) focused collection of only as much personal data as needed to accomplish stated purposes; and (7) accountability to consumers and enforcement authorities for compliance with the Consumer Privacy Bill of Rights.

The Privacy Blueprint calls on the federal government, under the leadership of the Department of Commerce, to convene and facilitate a multi-stakeholder process to develop enforceable codes of conduct for particular markets or industry sectors with significant consumer data privacy issues. Companies in a particular industry then may choose whether to adopt a particular code of conduct, and such commitment will be enforceable by the FTC under its existing authority. As an initial step in implementing this aspect of the Privacy Blueprint, NTIA issued a request for comment on the multistakeholder process to develop consumer data privacy codes of conduct, and specifically the "substantive consumer data privacy issues that warrant the development of legally enforceable codes of conduct, as well as procedures to foster the development of these codes."[111] The Privacy Blueprint also recommends inclusion of international stakeholders in the multi-stakeholder process for the development of codes of conduct discussed above, as well as international collaboration in global privacy investigations and enforcement actions.

C. Pending Legislation

The proliferation of mobile devices and LBS and the related consumer privacy concerns has not escaped the attention of 112th Congress. There has been significant interest on the issue

[111] 77 Fed. Reg. 13098 (Mar. 5, 2012).

of privacy from both the House of Representatives and Senate, with several significant privacy and information security-related bills introduced and numerous hearings held throughout the year. Individual members of Congress also have made inquiries to government agencies on specific aspects of consumer privacy.

Several bills addressing privacy issues have been introduced in the 112th Congress. In the Senate, S. 1223, the Location Privacy Protection Act of 2011, was introduced by Senator Al Franken (D-MN) in June 2011 and referred to the Judiciary Committee. The legislation proposes requiring affirmative opt-in consent before a covered entity could collect, receive, record, obtain, or disclose location information collected by electronic communication devices.[112] S. 1535, the Personal Data Protection and Breach Accountability Act of 2011, was introduced by Senator Richard Blumenthal (D-CT). This bill would enhance criminal and civil penalties for theft of personally identifiable information, including location data, and would require notification and remedies to affected consumers.[113] S. 1535 was reported out of the Senate Judiciary Committee on September 22, 2011. S. 799, the Commercial Privacy Bill of Rights Act of 2011, was co-sponsored by Senators John Kerry (D-MA) and John McCain (R-AZ). It instructs the FTC to create a comprehensive framework requiring entities collecting personally identifiable information to implement data security measures and provide clear notice of the collectors' practices and intended purpose of the collection.[114] Under the bill's proposed framework, individuals would have the right to opt-out of any collection and opt-in would be required for certain types of sensitive data. The bill would also require that individuals have access to and the ability to correct any personal information collected. S. 799 was referred to the Senate Committee on Commerce, Science, and Transportation on April 12, 2011.

---

[112] Location Privacy Protection Act of 2011, S. 1223, 112th Cong. (2011).

[113] Personal Data Protection and Breach Accountability Act of 2011, S. 1535, 112th Cong. (2011).

[114] Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011).

In the House of Representatives, Representative Bobby Rush (D-IL) introduced H.R. 611, the Building Effective Strategies to Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards ("BEST PRACTICES") Act.[115] Like S. 799, H.R. 611 instructs the FTC to develop a comprehensive framework requiring entities collecting covered personal and sensitive information to implement data security and notice practices. H.R. 611 also includes self-regulatory options for entities that meet certain FTC standards. Both S. 799 and H.R. 611 provide the FTC with authority to revise the definition of personally identifiable information. H.R. 611 extends the FTC rulemaking and enforcement authority over common carriers subject to the Communications Act, creating dual authority between the FTC and FCC with respect to privacy over common carrier networks. H.R. 611 was referred to the House Subcommittee on Commerce, Manufacturing, and Trade on February 18, 2011. On December 8, 2011 Representative Jose E. Serrano (D-NY) introduced a new bill "to require retail establishments that use mobile device tracking technology to display notices to that effect."[116] The bill, H.R. 3629, was referred to the House Committee on Energy and Commerce's Subcommittee on Commerce, Manufacturing, and Trade and instructs the FTC to enforce the Act under its unfair or deceptive trade practices authority.

Members of both the House and Senate have introduced separate "Do Not Track" legislation, which would give individuals the right to opt out of the collection, use, or sale of their online activities, including location based information. S. 913, the "Do-Not-Track Online Act of 2011,"[117] introduced by Senators Rockefeller (D-WV) and Pryor (D-AK), and H.R. 654, the "Do Not Track Me Online Act,"[118] introduced by Representatives Speier (D-CA), Hastings (D-FL) and Filner (D-CA), would direct the FTC to develop standards for an opt-out "do not track"

[115] BEST PRACTICES Act, H.R. 611, 112th Cong. (2011).

[116] H.R. 3629, 112th Cong. (2011).

[117] Do-Not-Track Online Act of 2011, S. 913, 112th Cong. (2011).

[118] Do Not Track Me Online Act, H.R. 654, 112th Cong. (2011).

mechanism. Failure to do so would be considered an unfair or deceptive practice under Section 5 of the FTC Act.[119] Under both bills the covered entity would have to disclose its collection and sharing practices, including with whom the consumer information is shared. Both would also allow the FTC to exempt commonly accepted commercial practices, such as the collection of information for billing purposes. H.R. 654 was referred to the House Subcommittee on Commerce, Manufacturing and Trade and S. 913 was referred to the Senate Commerce Committee.

The "Do-Not-Track For Kids" bill, H.R. 1895, sponsored by Representatives Markey (D-MA) and Barton (R-TX), would amend COPPA to require opt-in from the parent for children under 13 in order to collect location data. H.R. 1895 was referred to the House Subcommittee on Commerce, Manufacturing, and Trade on May 23, 2011.

While privacy issues generally have resonated on Capitol Hill, specific interest has generated around the issues of data security and data breach notifications. Representative Bono-Mack (R-CA) sponsored the "Secure and Fortify Electronic Data Act," (the "SAFE Data Act"), H.R. 2577, which requires the FTC to promulgate rules requiring data security and breach notification for entities that own or possess data containing personal information.[120] H.R. 2577's data security requirements do not apply to service providers with respect to third party electronic communications, and the bill limits the FTC's ability to alter the scope of data defined as "personal information" and therefore protected under the Act. The bill was referred to the Subcommittee on Commerce, Manufacturing, and Trade on July 29, 2011.

Other data security bills in the House include the "Data Accountability and Trust Act," H.R. 1707,[121] introduced by Representative Rush (D-IL), and the "Data Accountability and Trust Act (DATA) of 2011," H.R. 1841, sponsored by Representatives Stearns (R-FL) and Matheson

[119] 15 U.S.C. § 45.

[120] The SAFE Data Act, H.R. 2577, 112th Cong. (2011).

[121] Data Accountability and Trust Act, H.R. 1707, 112th Cong. (2011).

(R-UT).[122] Representatives Stearns and Matheson also introduced H.R. 1528, "The Consumer Privacy Protection Act of 2011,"[123] which is intended to provide consumers with comprehensive privacy protection concerning the use and sharing of their personal information, would apply to all non-governmental entities, and would give the FTC sole enforcement authority. All three bills have been referred to the House Subcommittee on Commerce, Manufacturing, and Trade.

In the Senate, S. 1207, the "Data Security and Breach Notification Act of 2011," sponsored by Senators Pryor (D-AK) and Rockefeller (D-WV), similarly requires the FTC to promulgate rules requiring data security and breach notification for entities that own or possess data containing personal information.[124] S. 1207 was referred to the Senate Commerce Committee on June 15, 2011 and no further action has occurred.

VIII. CONCLUSION

Location-based services are transforming the ways people across the country conduct business, organize their lives, and have fun. They can save time, money, and even lives. However, because of the technologies that enable them, LBS have the inherent ability to create accurate snapshots of their users' activities that can contain very personal information. As both the potential and the challenges of LBS have become more understood, the Commission, along with other federal agencies and Congress, has begun to assess ways to best ensure the LBS users enjoy all their benefits and that their confidential information is secure. Industry has also played an important role.

The Commission has a long tradition of ensuring that the privacy of consumers is protected. The Commission's consistent goals have been: ensuring that personal information is protected from misuse and mishandling, requiring providers to be transparent about their practices, and enabling consumer control and choice. This has helped inform Commission

[122] Data Accountability and Trust Act (DATA) of 2011, H.R. 1841, 112th Cong. (2011).

[123] The Consumer Privacy Protection Act of 2011, H.R. 1528, 112th Cong. (2011).

[124] Data Security and Breach Notification Act of 2011, S. 1207, 112th Cong. (2011).

activities with respect to LBS, which have included a day-long forum on LBS benefits and challenges, close collaboration with other federal agencies and Congress, and constructive interaction with industry.

The potential of LBS to provide value and foster innovation to benefit the economy and consumers is tremendous. It is clear that there are also threats to consumers' legitimate interest in protecting their personally identifiable information, in particular from the lack of clear and consistent disclosure about how that information is being collected, safeguarded and used by location-based services. While industry is taking steps to minimize these threats, the degree of responsiveness varies, new issues continue to emerge, and LBS industry players face challenges as they attempt to provide consumers with appropriate notice and choice. Nonetheless, there is room for additional steps to be taken, particularly with respect to less established LBS providers, to ensure growing concerns are addressed as quickly and as comprehensively as possible—and at all levels of industry. Issues to consider include:

- **Consideration of Privacy Issues at Earliest Stages of Product Development.** What are the most effective means to ensure privacy considerations become an integral part of the product design and development process for all players in the LBS industry? What should consumers be told?
- **Security of data**. What are the rights, duties, and obligations of the parties that generate, aggregate, or hold LBS-related data to secure such data from unauthorized disclosure or access? Do they vary as a result of a party's relationship with the customer?
- **Timing and sufficiency of notice.** How much information should be pushed to consumers at different points in their interaction with an LBS, mobile, application or other provider and how should it be presented? Must the information be provided each time an application or service is used? Should there always be an opt out?

- **Data Minimization.** Should parties be encouraged to collect the minimal amount of data technically required to provide a location-based service and retain that data for the minimum amount of time necessary?

Engagement between government and industry will be essential to ensure there is an appropriate balance between the benefits of LBS technology and its challenges to user privacy. The Commission should continue to work closely with its federal partners and industry representatives to empower consumers, encourage transparency, and protect confidential data. In particular, the Commission should continue to monitor industry compliance with applicable statutory requirements and evolving industry best practices. Additional steps may be necessary if privacy issues are not met as effectively and comprehensively as possible or within reasonable time frames.

APPENDIX A

Commenters in WT Docket No. 11-84

American Civil Liberties Union ("ACLU"), Speech, Privacy, and Technology Project of the ACLU and the ACLU of Northern California
AT&T Inc.
Center for Democracy & Technology
Direct Marketing Association
Google Inc.
Interactive Advertising Bureau
Privacy Rights Clearinghouse
TechAmerica
The NetChoice Coalition
True Position, Inc.
Verizon Wireless
Wahab & Medenica LLC

APPENDIX B

AGENDA
Helping Consumers Harness the Potential of Location-Based Services

9:00 a.m. **Welcome and Opening Remarks**
- Rick Kaplan, Chief, Wireless Telecommunications Bureau

9:05 a.m. **An Overview of Location-Based Services and Technologies**
- Matt Blaze, Associate Professor, University of Pennsylvania

9:30 a.m. **Panel 1: Trends in Location-Based Services**
In this panel, carriers and application developers will discuss the types of Location-Based Services currently being offered, potential new Location-Based Services offerings that are in development, and general usage trends. In addition, the panel will discuss the business and technological interactions between carriers and application developers.

Moderators:
- Edward Felten, Chief Technologist, Federal Trade Commission
- John Leibovitz, Deputy Bureau Chief, Wireless Telecommunications Bureau, Federal Communications Commission

Panelists:
- Alan Chapell, Chairman of the Mobile Marketing Association's Privacy and Preferences Committee and Founder of Chapell & Associates
- Kristi Crum, Executive Director – Consumer Solutions
  Verizon Wireless
- Alan Davidson, Director of Public Policy for the Americas, Google Inc.
- Carter Griffin, General Partner, Updata Partners
- Tim Sparapani, Director of Public Policy, Facebook
- Brandt Squires, Consultant, Squirebend LLC (previously Director Livingsocial, Co-founder BuyYourFriendADrink.com)
- Jon Steinback, Director of Marketing, Foursquare Labs, Inc.

11:00 a.m. **Break**

11:15 a.m. **Panel 2: Company-Based Approaches to Protect Privacy**
Panelists will discuss measures the industry is taking to protect consumer privacy, establish industry best practices, and develop privacy-enhancing technologies. The panel will discuss the ways in which companies provide information about their privacy policies to consumers, such as the usage of consumer privacy notices and the type of information typically disclosed in these notices.

Moderators:
- Charles Mathias, Assistant Chief, Wireless Telecommunications Bureau
- Douglas Sicker, Chief Technologist, Federal Communications Commission

Panelists:

- Justin Brookman, Director, Project on Consumer Privacy, Center for Democracy and Technology
- Maureen Cooney, Deputy Chief Privacy Officer, Director of Office of Privacy, Sprint Nextel
- Lorrie Cranor, Associate Professor, Computer Science and Engineering and Public Policy, Carnegie Mellon University
- Ted Morgan, Founder and CEO, Skyhook Wireless
- Patti Poss, Counsel to the Director of the Bureau of Consumer Protection, Federal Trade Commission
- Scott Taylor, Chief Privacy Officer, Hewlett Packard

12:45 p.m. **Break**

1:15 p.m. **Lunch Presentation by Chief Richard Price, San Ramon CA Fire Protection District**

1:45 p.m. **Panel 3: Protecting Your Privacy – What Consumers and Parents Should Know**

This panel will provide an overview of steps consumers can take now to protect their privacy when using Location-Based Services. The panel will provide consumer DOs and DON'Ts, and provide information on what parents should know about location tracking when their children use mobile devices.

Moderators:

- Joel Gurin, Chief, Consumer and Governmental Affairs Bureau
- Jennifer Tatel, Associate General Counsel, Office of General Counsel

Panelists:

- Michael Altschul, General Counsel, CTIA-The Wireless Association®
- Dr. Edward G. Amoroso, Senior Vice President and Chief Security Officer, AT&T Services, Inc.
- Stephen Balkam, CEO, Family Online Safety Institute
- Brendon Lynch, Chief Privacy Officer, Microsoft
- Alan Simpson, Vice President of Policy, Common Sense Media
- Nat Wood, Assistant Director, Division of Consumer and Business Education, Bureau of Consumer Protection, Federal Trade Commission

3:00 p.m. **Closing Remarks**

- Peter Swire, C. William O'Neill Professor of Law, Moritz College of Law of the Ohio State University

3:15 pm **Adjourn**