

Public Workshop:

**The Mobile Wireless
Web, Data Services
and Beyond:**

**Emerging
Technologies and
Consumer Issues**

Federal Trade Commission
February 2002

Contents

- I. Introduction 1

- II. Overview of Wireless Technology 2
 - A. Background on Wireless Internet and Data Technologies 2
 - B. Location-Based Services and Advertising 4
 - C. Challenges for the Wireless Industry 6

- III. Privacy Issues 8
 - A. Privacy Concerns 8
 - B. Addressing Privacy Concerns in the Wireless Space 13

- IV. Security Concerns 13

any Conc

I. Introduction

Wireless technologies are opening up many new opportunities for consumers. Wireless Internet technologies provide access to the wireless World Wide Web (“Web”), allowing consumers to obtain valuable information and engage in fast and efficient commercial transactions. Wireless data technologies, such as instant messaging and Short Message Service (“SMS”) systems, allow consumers to communicate anytime, and from many locations. However, the growth of these technologies has also raised privacy, security, and other consumer protection issues.

On December 11 and 12, 2000, the Federal Trade Commission (“FTC”) held a public workshop to educate itself and the public about emerging wireless technologies and to provide a forum for discussion of the consumer protection issues raised by these technologies.¹ The workshop provided a wealth of information on these issues and opened a dialogue between the Commission and a wide range of interested parties – common carriers that provide wireless services, wireless content providers, location information generators, application service providers, equipment makers, direct marketers, consumer advocates, and trade associations.

During the workshop, numerous industry experts and consumer advocates gave informative presentations and participated in panel discussions. This report summarizes the issues discussed during the workshop. It highlights areas of consensus and records the issues upon which participants did not agree. It is a resource for readers who want to learn more about emerging wireless technologies and the consumer protection issues they raise.

The workshop was organized into five basic topic areas: (1) an overview of the technologies and the issues raised by them; (2) privacy issues; (3) security issues; (4) advertising and disclosures; and (5) self-regulatory programs. On the first day of the workshop, participants described the wireless technologies available;² they also discussed the future of wireless capabilities,³ the business models for providing information and engaging in m-commerce (the term used to denote mobile electronic commerce), and the nature of consumer relationships with wireless service providers.⁴ Participants also considered the opportunities and challenges that the industry faces in developing successful wireless applications in the U.S. market.⁵

¹ This report was prepared by Allison Brown and Jessica Rich of the FTC staff. It does not necessarily reflect the views of the Commission or any individual Commissioner.

² Transcript, December 11, 2000, at 10-23. Unless noted otherwise, footnote citations are to the transcript of the Workshop, which is available online at <http://www.ftc.gov/bcp/workshops/wireless/>. Footnotes that cite to specific panelists identify the panelist’s last name, the organization that the panelist represented at the workshop, and the page number where the statement is located in the transcript. The complete list of Workshop participants can be found in Appendix A.

³ *Id.* at 24-90.

⁴ *Id.* at 91-143.

⁵ *Id.* at 143-79.

⁶ *Id.*, December 12, 2000, at 186-239. In addition, a representative from the Federal Communications

programs, games, and Web portals.¹⁴ One workshop participant explained that if the consumer requests a weather forecast on a mobile phone, for example, the consumer can view a text-based forecast on the mobile phone screen without all of the rich graphics that the consumer would be likely to see on the wired Web.¹⁵

Wireless data technologies include instant messaging, paging technology, and SMS messages (text messages transmitted over the wireless network and displayed on wireless phones). SMS systems enable subscribers to receive voicemail notification, digital pages, personal messages, and informational services like stock quotes, sports scores, weather, and traffic.¹⁶

Consumers are now able to access the wireless Web and use wireless data services through various devices, including mobile phones, pagers, two-way radios, and personal digital assistants (“PDAs”). The type of device a consumer uses affects the type of information and content that the consumer can receive. For example, one workshop participant explained that a PDA with a large screen may be better than a mobile phone for reviewing emails and accessing the wireless Web.¹⁷ Another panelist stated that car-based devices (also called “in-vehicle information systems”) allow people to access numerous wireless services in their cars.¹⁸ These devices typically have larger screens and more features than mobile phones.¹⁹ A panelist also stated that manufacturers are developing hybrid devices that combine features of mobile phones and PDAs to allow consumers to access voice services and data services from a single device.²⁰ In 2001, manufacturers introduced several of these hybrid PDA-cell phones, which were generally larger than regular cellular phones and had lower voice quality.

¹⁴ See Mossberg, *The Wall Street Journal*, at 16-17.

¹⁵ Bodin, IBM Pervasive Computing Division, at 40.

¹⁶ The most popular mobile product in Europe is SMS messaging. Pavona, Terra Lycos, at 80.

¹⁷ Mossberg, *The Wall Street Journal*, at 18.

¹⁸ Bodin, IBM Pervasive Computing, at 27.

¹⁹ *Id.*

²⁰ Mossberg, *The Wall Street Journal*, at 18.

²¹ See Ben Charny, *Nokia Ships Combo PDA-Cell Phone*, CNET News.com, at <http://news.cnet.com/news/0-1004-200-6322274.html> (June 19, 2001); see also Ian Fried, *Handspring's PDA-Phone Close At Hand*, CNET News.com, at <http://news.cnet.com/news/0-1006-200-7850726.html> (November 12, 2001).

²² See David Pogue, *Doing It All: One Gadget, Tried Twice*, N.Y. TIMES, January 3, 2002 at G1.

B. Location-Based Services and Advertising

Location-based services and advertising allow consumers to receive services and advertising based on their geographic location. For example, businesses can provide information about traffic, restaurants, retail stores, travel arrangements, or automatic teller machines based on the consumer's location at a particular moment in time.²³ Such services can be provided in response to a consumer's manual input of his or her location information into the handset or by using so-called "auto-location" technology to track the location of the consumer automatically.²⁴

Some panelists at the workshop stated that general location information, such as the town in which the user lives, would be sufficient for many location-based services.²⁵ For example, the consumer could go to a wireless Web site and request information about the weather forecast for the user's home city.²⁶ Or a user viewing a clothing retailer's advertisement on a PDA could enter a zip code to find the nearest store.²⁷ Other location-based services require that the business know the consumer's precise location at a given time. With this information, for example, as a person passes a store, a merchant could call the consumer or send an SMS message to notify the consumer of a sale.²⁸

"Auto-location" technologies, mentioned above, will soon allow the automatic physical tracking of a user's location so that a consumer can receive location-based services and advertising without manually inputting a location. The primary technologies for such auto-location services are 1) network-based triangulation systems, 2) Global Positioning System ("GPS") devices, and 3) hybrid systems. A network-based triangulation system collects radio signals at the three cell towers closest to the user and then uses the locations of those cell towers to compute the user's exact location.²⁹ The GPS is a set of twenty-four specially placed satellites that continuously transmit their position. Where a GPS processor is embedded in a phone handset, the handset can process GPS information from the satellites and then send the information back to a device on the network to determine the user's position.³⁰ A hybrid system utilizes a combination of the two technologies.

²³ Pollard, Expedia.com, at 281; Stutman, ClickaDeal.com, at 285-86; Weisler, Vindigo Company, at 282; Assenzo, Sprint PCS, at 283.

²⁴ See Weisler, Vindigo Company, at 282.

²⁵ Pollard, Expedia.com, at 290; Assenzo, Sprint PCS, at 290-91.

²⁶ See Bodin, IBM Pervasive Computing, at 40.

²⁷ Harrison, Windwire, at 404.

²⁸ See Ponemon, Guardent, Inc., at 192.

²⁹ Amarosa, True Position, Inc., at 255.

³⁰ Neihardt, QUALCOMM, Inc., at 260.

Workshop participants whose companies generate auto-location data provided examples of a network-based system and a hybrid system. A representative of True Position, Inc., a company that operates a network-based auto-location system, stated that the company calculates the user's position using the locations of the three nearest cell towers and then delivers the location records to content providers previously authorized by the consumer to provide location-based services.³¹ A representative of QUALCOMM, Inc. gave an example of a hybrid system, called SnapTrack, that combines network-based triangulation technology and GPS technology in order to increase the reliability and accuracy of location information.³² In the SnapTrack system, the user's position is calculated using both the GPS data and network-based information.³³ The auto-locate feature is only activated upon the manual command of the user,³⁴ either when the user dials 911 for emergency services or deliberately activates a location-enabled feature.³⁵

Panelists also discussed the use of a location information gateway in conjunction with auto-location technology. A location information gateway collects location information from users and then sends various types of messages to users from different merchants. A representative of Invertix Corporation stated that it launched a commercial gateway for wireless carriers in Europe and Asia in 2000.³⁶ The gateway gathers wireless subscriber location information from carriers' network signals and then sends coupons and messages to subscribers from merchants they select.³⁷ Subscribers provide personal information and establish the conditions under which they are willing to be contacted by third parties on Invertix's Web site.³⁸ For example, a subscriber can determine whether the carrier may provide information to third parties about whether the user's device is on, or where the user is at any given moment.³⁹ The user can select specific companies to have access to the location information, and he or she can indicate "blackout times" when he or she does not want to be

³¹ Amarosa, True Position, Inc., at 256.

³² Neihardt, QUALCOMM, Inc., at 261. Neihardt expected that QUALCOMM would employ this technology first in Japan during the first half of 2001, and in the U.S. and Korea shortly after that. *Id.* at 264.

³³ *Id.* at 261.

³⁴ *Id.* at 261.

³⁵ *Id.* at 263.

³⁶ Hurtado, Invertix Corporation, at 267.

³⁷ *Id.* at 268-70.

³⁸ *Id.* at 269.

³⁹ *Id.* 270.

⁴⁰ ARTHUR HURTADO, INVERTIX I-M ANYWHERE: FEDERAL TRADE COMMISSION PANEL: GENERATION AND CONTROL OF LOCATION INFORMATION 6-8 (2000), <http://www.ftc.gov/bcp/workshops/wireless/presentations/hurtado.pps> (Power Point Presentation).

⁴¹ *Id.*

⁴² *Id.* at 3.

⁴³ Bob Brewin, *Sprint PCS Debuts GPS-Equipped Wireless Phone For 911 Calls*, Computerworld, at http://www.computerworld.com/itresources/rcstory/0,4167,STO64380_KEY68,00.html (October 1, 2001).

⁴⁴ VERIZON WIRELESS, E911 STATUS E911

⁴⁹ Mossberg, *The Wall Street Journal*, at 20-21.

⁵⁰ The standards include analog cellular, global system for mobile communications, code division multiple access, and time division multiple access. For a description of these technologies, see <http://www.wow-com.com/consumer/howitworks/>.

⁵¹ Mossberg, *The Wall Street Journal*, at 22-23.

⁵² *Id.* at 22.

⁵³

⁷⁵ Schlichting, FCC, at 245. The original deadline for carriers to begin using precise location technology was October 1, 2001. However, five nationwide carriers petitioned to modify the deadline, and on October 5, 2001, the FCC conditionally approved their requests to modify the schedule but re-affirmed that all carriers and call centers must fully complete the implementation of auto-location technology by December 31, 2005. *See* FEDERAL COMMUNICATIONS COMM'N, FCC ACTS ON WIRELESS CARRIER AND PUBLIC SAFETY REQUESTS REGARDING ENHANCED WIRELESS 911 SERVICES (2001),

The Mobile Wireless Web, Data Services and Beyond

⁹⁹ Davidson, Center for Democracy and Technology, at 206; Bromley, Fiderus Strategic Security and Privacy Services, at 207.

¹⁰⁰ Ponemon, Guardent, Inc., at 235-36; *see* Cranor, AT&T Labs-Research, at 204.

¹⁰¹ *See, e.g.*, Ponemon, Guardent, Inc., at 235-36; Lucas, Persona, Inc., at 411; *see also* Mossberg, The Wall Street Journal, at 12; Stutman, ClickaDeal.com, at 300. As noted at the workshop, U.S. consumers must pay for incoming wireless calls. Pavona, Terra Lycos, at 76.

¹⁰² Davidson, Center for Democracy and Technology, at 207.

¹⁰³ Ponemon, Guardent, Inc., at 235-36.

¹⁰⁴ Altschul, CTIA, at 372; *see also* Davidson, Center for Democracy and Technology, at 199; Bromley, Fiderus Strategic Security and Privacy Services, at 202.

¹⁰⁵ *See, e.g.*, Davidson, Center for Democracy and Technology, at 199; Ponemon, Guardent, Inc., at 198;

characters of text to be seen at a time, and PDA screens are relatively small as well.¹⁰⁷ Thus, the tension between writing a comprehensive privacy policy and a policy that is concise and understandable will be exacerbated in the wireless space.¹⁰⁸

Panelists suggested that carriers, at least, can make privacy disclosures in the initial service contracts for wireless devices.¹⁰⁹ Web sites and other content providers, however, may or may not require consumers to sign service contracts before providing services.¹¹⁰ Panelists discussed some technologies that could help both carriers and content providers to provide effective notice. Some noted that “call-through” technology – which allows a cellular phone user to click a link on a wireless Web site that automatically dials a phone number and connects the user to a live person or a recording – may be useful in providing privacy disclosures.¹¹¹ A representative of the privacy self-regulatory group, TRUSTe, also suggested that a combination of symbols, call-through technology, and disclosures in the wireless service contract could provide adequate privacy disclosures for wireless services.¹¹² He cautioned, however, that a site that relied on audio disclosures would have to provide a mechanism for recording a written version of the stated policy on the date the consumer used the service, as well as provide a dispute resolution process, since a voice-based policy would not be a permanent mechanism.¹¹³

A panelist from an Internet advertising company stated that privacy disclosures should be posted in several different places, and they s

¹⁰⁷ See Peters, Lot21, Inc., at 401.

¹⁰⁸ Lewin, TRUSTe, at 425-26.

¹⁰⁹ *Id.* at 435; Cranor, AT&T Labs - Research, at 203.

¹¹⁰ See Harrison, Windwire, at 404 (example where consumer calls restaurant reservation service without signing initial contract).

¹¹¹ Lewin, TRUSTe, at 434-35; Harrison, Windwire, at 404.

¹¹² Lewin, TRUSTe, at 434-35.

¹¹³ *Id.* at 438.

¹¹⁴ Moore, 24/7 Media, Inc., at 232.

¹¹⁵ Lucas, Persona, Inc., at 431-32.

¹¹⁶ *Id.*

registers for the service on a wired Internet site; in those instances, the consumer could first review the privacy policy on a larger screen on the wired Internet site.¹¹⁷

Panelists also agreed that consumers should be given some choice about the collection and use of their information in the wireless space.¹¹⁸ Panelists stated that consumers will not like unsolicited messages on their wireless devices, although many pane

¹¹⁷ Peters, Lot21, Inc., at 433.

¹¹⁸ Moore, 24/7 Media, Inc., at 197; Ponemon, Guardent, Inc., at 198; Davidson, Center for Democracy and Technology, at 199.

¹¹⁹ Donahue, American Association of Advertising Agencies, at 409-10; Peters, Lot21, Inc., at 410-11; Lucas, Persona, Inc., at 411-12; Mossberg, The Wall Street Journal, at 12.

¹²⁰ Harrison, Windwire, at 409; *id.* at 413. For a more detailed definition of push advertising, see WIRELESS ADVERTISING ASS'N, WAA GUIDELINES ON PRIVACY AND SPAM § II(C) (2000), http://www.waaglobal.org/press/privacy_press.html [hereinafter WAA/MMA GUIDELINES].

¹²¹ Harrison, Windwire, at 413; *see also* Moore, 24/7 Media, Inc., at 208. For a more detailed definition of pull advertising, *see* WAA/MMA GUIDELINES § II(D).

¹²² Moore, 24/7 Media, Inc., at 197.

¹²³ Assenzo, Sprint PCS, at 298; Stutman, ClickaDeal.com, at 302.

¹²⁴ Hendricks, Privacy Times, at 303-04; *see also* Davidson, Center for Democracy and Technology, at 231.

in emergencies).¹²⁵ A representative of ClickaDeal.com, a company that plans to provide location-based coupons, suggested that companies routinely purge users' location information. He stated that his company plans to cleanse its logs of user location information every hour so that it does not retain a history of a consumer's physical movements.¹²⁶

A representative of the Center for Democracy and Technology cautioned that ensuring meaningful choice in the wireless environment will be challenging for several reasons.¹²⁷ First, the consumer may not know exactly what parties are potentially receiving personal information, because carriers, advertisers, and other service and content providers may be involved but not visible to consumers.¹²⁸ Second, even opt-in consent, if it is provided only at the initial point in time when a consumer signs a service contract, and not at the point of information collection, may not be adequate; this is especially true if the privacy disclosures are not clear and easy to understand.¹²⁹ The panelist stated rather than debating the concept of opt-in versus opt-out consent, companies should try to achieve informed consent that truly gives consumers control over their personal information.¹³⁰

Panelists agreed that manufacturers, carriers, content providers, and software developers will have to work together to enable effective notice and choice for consumers.¹³¹ Panelists also briefly discussed whether consumers should be given access to the information collected about them for review, correction, and/or deletion. Panelists stated that this is a complicated issue that raises difficult problems, such as how companies can authenticate users that request access to their information.¹³² Finally, panelists agreed that consumer education is an important component of protecting consumer privacy.¹³³

2. Building Privacy Solutions into the Technological Architecture

There was general consensus that technology can help improve privacy in the wireless space in numerous ways. Panelists suggested that implementation of the Platform for Privacy Preferences ("P3P"), a set of software-writing guidelines developed for the wired Internet by

¹²⁵ Hendricks, *Privacy Times*, at 304.

¹²⁶ Stutman, *ClickaDeal.com*, at 301.

¹²⁷ Davidson, *Center for Democracy and Technology*, at 200.

¹²⁸ *Id.*; *see also* Ponemon, *Guardent, Inc.*, at 199.

¹²⁹ Davidson, *Center for Democracy and Technology*, at 200; *see also* Moore, *24/7 Media, Inc.*, at 232.

¹³⁰ Davidson, *Center for Democracy and Technology*, at 231.

¹³¹ *Id.* at 210; Cranor, *AT&T Labs - Research*, at 211-12; Bromley, *Fiderus Strategic Security and Privacy Services*, at 212.

¹³² Davidson, *Center for Democracy and Technology*, at 228; Bromley, *Fiderus Strategic Security and Privacy Services*, at 228.

¹³³ Moore, *24/7 Media, Inc.*, at 213; Davidson, *Center for Democracy and Technology*, at 238.

the World Wide Web Consortium, would be useful to consumers in the wireless space.¹³⁴ P3P provides a language to express privacy policies in a machine-readable format. If P3P were implemented on wireless Web sites, a site would be able to express its information practices in P3P, and a P3P-enabled browser could read the P3P-enabled policy; thus, a user would not have to read a privacy policy on the device's small screen.¹³⁵

Beyond P3P, panelists also discussed a digital rights management approach, which would enable consumers to determine specifically what parties had access to their data, and provide technology so that consumers' permissions could be attached to their data.¹³⁶ A representative of Nextel Communications stated that privacy could be enhanced by the use of a proxy or agent that acts on the user's behalf to enable previously set privacy preferences.¹³⁷ A representative from Microsoft Corporation expressed support for "persona management," which would allow a user to provide different privacy preferences for Web browsing at different times.¹³⁸ For example, a consumer could choose to be a "work persona" and provide only work contact information; a "home persona" and provide only home contact information; or an "anonymous persona" so that no personal information would be transmitted.¹³⁹

IV. Security Concerns

Some panelists also expressed concern about the security of data transmitted through wireless devices.¹⁴⁰ Panelists explained that although the public has the perception that wireless communications are vulnerable to interception over the airwaves, the risk of such eavesdropping is in fact very small.¹⁴¹ The more significant vulnerability exists within the carrier networks, especially at the point where the transmissions are translated from the wireless protocol (a set of rules governing wireless communications) to the wireline protocols

¹³⁴ Ponemon, Guardent, Inc., at 198; Cranor, AT&T Labs - Research, at 203; Davidson, Center for Democracy and Technology, at 206; LeMaitre, Nextel Communications, Inc., at 336-37.

¹³⁵ To date, P3P technology is not available on any wireless Web sites. While some wireless companies are actively experimenting with P3P, none has made a public commitment to implement P3P technology in the wireless space. Telephone Interview with Lorrie Cranor, Principal Technical Staff Member, AT&T Labs - Research (November 13, 2001).

¹³⁶ Purcell, Microsoft Corporation, at 352; Miller, MEconomy, Inc., at 353; Smith, Privacy Foundation, at 358-9; see LeMaitre, Nextel Communications, Inc., at 346-47.

¹³⁷ LeMaitre, Nextel Communications, Inc., at 328. For additional information about Web agents, see XNS PUBLIC TRUST ORGANIZATION, *How Web Agents Work: A Primer* (2002), <http://www.xns.org/xns/whitepapers/webagents/>.

¹³⁸ Purcell, Microsoft Corporation, at 329-30.

¹³⁹ *Id.*

¹⁴⁰ Cranor, AT&T Labs - Research, at 204.

¹⁴¹ Bromley, Fiderus Strategic Security and Privacy Services, at 215.

3) only using data collected for a transaction for the specific transaction at hand.¹⁵² Other suggestions for improving wireless security were the implementation of authentication using public key infrastructure¹⁵³ and the implementation of Wireless Transport Layer Security.¹⁵⁴ In Europe, a standards working group is developing a small graphic that could be displayed on a phone to show that the transaction is secure, and one participant stated that this approach could be useful in the U.S. as well.¹⁵⁵

A panelist stated that if consumers purchase items over their mobile devices with a payment mechanism other than a credit card, such as billing a transaction directly to a consumer's wireless phone bill, the purchases are not protected by the Fair Credit Billing Act;

¹⁵² *Id.* at 324.

¹⁵³ Edgar, *Diversinet*, at 331.

¹⁵⁴ Miller, *MEconomy, Inc.*, at 333.

¹⁵⁵ Bergeron, *Zero-Knowledge Systems, Inc.*, at 350.

¹⁵⁶ 15 U.S.C. § 1643 (1994).

¹⁵⁷ *See* Saunders, *National Consumer Law Center*, at 163-64.

¹⁵⁸ *Id.*

¹⁵⁹ Peters, *Lot21, Inc.*, at 400; Harrison, *Windwire*, at 403.

¹⁶⁰ Peters, *Lot21, Inc.*, at 403.

¹⁶¹ *See* Harrison, *Windwire*, at 419-20.

¹⁶² *Id.* at 404.

stated that voice-based advertisements may be the most effective advertising tool on cellular phones.¹⁶³ Another panelist stated that the most effective advertising on cellular phones will be short, text-only messages.¹⁶⁴

Panelists also described the different formats that are available for wireless advertisements. Advertisers can include a promotional message when they provide information requested by a consumer; for example, they can include a logo for a sporting goods store along with a requested SMS notification about tickets to a sporting event.

¹⁶³ Donahue, American Association of Advertising Agencies, at 416; Harrison, Windwire, at 419-20; Peters, Lot21, Inc., at 421-22.

¹⁶⁴ Peters, Lot21, Inc., at 407.

¹⁶⁵ Harrison, Windwire, at 406.

¹⁶⁶ *See id.* at 404.

¹⁶⁷ *Id.* at 405.

¹⁶⁸ *See* Peeler, Federal Trade Commission, at 423.

¹⁶⁹ *See* Lewin, TRUSTe, at 424-25; Harrison, Windwire, at 429-30; Lucas, Persona, Inc., at 431.

¹⁷⁰ Harrison, Windwire, at 430.

¹⁷¹ Peters, Lot21, Inc., at 433.

A. Cellular Telecommunications and Internet Association

The CTIA represents cellular carriers, Personal Communication Service carriers, telecommunications vendors, wireless application service providers, data developers, and wireless device manufacturers.¹⁷⁹ A CTIA representative stated at the workshop that the CTIA developed principles to provide consumers with a uniform set of privacy expectations for the use of consumers' location information.¹⁸⁰ It has petitioned the FCC requesting that the agency formally adopt the guidelines as a safe harbor from enforcement against carriers under the Telecommunications Act.¹⁸¹ The organization plans to wait for the FCC to adopt final regulations governing location information privacy before adopting a self-regulatory program for its members.¹⁸² If the CTIA eventually adopts the FCC rules as self-regulatory guidelines, the guidelines would apply to service providers that are not common carriers covered by the FCC's rules, as well as to common carriers.¹⁸³

CTIA's proposed location privacy guidelines require service providers to ensure that 1) customers are well-informed of location information collection and use before collection; 2) consumers have a meaningful opportunity to consent to the collection and use of information for location-based services; and 3) consumers are assured of the security and integrity of the location-based information.¹⁸⁴

The CTIA principles provide three examples of methods that can be used to make the required disclosures to customers about location information practices: 1) include the notification in a service agreement before the commencement of the services; 2) provide a description of location information policies through electronic mail, on a Web site, or in a letter sent to subscribers; or 3) provide notice on a bill directing subscribers to a toll-free number or an Internet site address for a description of the carrier's complete policies and practices.¹⁸⁵

¹⁷⁹ Altschul, CTIA, at 373.

¹⁸⁰ *Id.* at 375.

¹⁸¹ As discussed above, common carriers, many of whom are members of the CTIA, must comply with a statute requiring that they obtain "express prior authorization" from a consumer before releasing location information to third parties. See 47 U.S.C. § 222(f). The CTIA petition requests a rulemaking to implement this statutory mandate and adopt the CTIA's proposed privacy guidelines as a safe harbor from FCC enforcement actions for any common carrier that follows the principles. CELLULAR TELECOMMUNICATIONS AND INTERNET ASS'N, CTIA REQUEST TO COMMENCE RULEMAKING TO ESTABLISH FAIR LOCATION INFORMATION PRACTICES 3 (2000), <http://www.wow-com.com/pdf/ctia112200.pdf>. If the FCC establishes such regulations, a carrier's failure to implement the safe harbor principles, or failure to abide by the safe harbor principles, could subject it to enforcement actions under the FCC's rules. Altschul, CTIA, at 377.

¹⁸² Telephone Interview with Michael Altschul, Vice President/General Counsel, CTIA (February 14, 2002).

¹⁸³ *Id.*

¹⁸⁴ *Id.* at 376-77.

¹⁸⁵ *Id.* at 9.

The CTIA's proposed rules are flexible as to how meaningful consent can be obtained, but state that the consent must be "manifest and express" before location information can be used.¹⁸⁶ The principles also provide examples of methods to obtain consent. One example is obtaining the consent through a signed service agreement before the commencement of the services.¹⁸⁷ Another example is to obtain consent through a "clickwrap" agreement (a mechanism that allows a consumer to assent to the terms of a contract by "clicking" on an acceptance button on a Web site).¹⁸⁸

As currently proposed, the guidelines do not provide any additional guidance on the format or content of these methods for providing notice and choice. Therefore, it is not clear whether and how some of these methods will satisfy the guidelines' general principles to ensure that customers are "well-informed" and have a meaningful opportunity to provide "manifest and express" choice. In particular, additional guidance may be needed to ensure that important privacy disclosures are not buried in a long agreement, letter, email, or phone bill, and that choice is not then gleaned from the signing of the agreement, purchase of a subscription, or the "click" of a button on a Web site. As panelists stated at the workshop, privacy disclosures are meaningful only if they are clear, easy to read, and understandable.¹⁸⁹ Thus, where disclosures are made in a telephone bill, service agreement, or other long document, it is important that they be made in a place and in a format that calls sufficient attention to them.¹⁹⁰

In discussions with FTC staff about this issue since the workshop, CTIA representatives agreed that notice that is buried in the back of a long service agreement, or placed in small print on a telephone bill, would not generally ensure that the consumer was "well-informed" as required by the guidelines.¹⁹¹ Accordingly, if the guidelines are adopted, the FTC staff encourages CTIA to provide additional guidance to its members on the issue of clear and conspicuous disclosures as the companies bring location-based products and services to consumers.¹⁹² The FTC staff also encourages CTIA to consider adopting its principles as a self-regulatory program, even in the absence of formal recognition in the FCC's rules.

¹⁸⁶ *Id.* at 10.

¹⁸⁷ *Id.*

¹⁸⁸ *Id.*

¹⁸⁹ Davidson, Center for Democracy and Technology, at 206; Moore, 24/7 Media, Inc., at 232; Ponemon, Guardent, Inc., at 209; Cranor, AT&T Labs-Research, at 234; Stutman, ClickaDeal.com, at 309-310.

¹⁹⁰ Recently, the FTC and seven other agencies held a workshop to explore strategies for providing effective notice under the Gramm-Leach-Bliley Act. As discussed at the workshop, some of the strategies include effective use of headings, space, and other visual design features to ensure the clarity and prominence of important disclosures. Transcript, *Get Noticed: Effective Financial Privacy Notices*, December 4, 2001, at 163-64, available at <http://www.ftc.gov/bcp/workshops/glb/index.html>.

¹⁹¹ Discussion with Michael Altschul, Vice President/General Counsel, CTIA (August 22, 2001).

¹⁹² *Id.*

communication to an email address. Halpert, *The Direct Marketing Ass'n*, at 394.

²⁰² WAA/MMA G

Since the workshop, the WLIA has written privacy guidelines for its members setting standards to govern the use and compilation of personally identifiable location data.²⁰⁹ The guidelines require, among other things, that each WLIA member adopt a privacy policy that is readily available to consumers at the time that they consider or agree to participate in any location-based service.²¹⁰ The standards require that the privacy policy must be clear and conspicuous, as well as easy to find, read, and understand, “to the point that no prospective subscriber would be likely to reach the point of subscription without being confronted with an invitation to review the privacy policy.”²¹¹ The privacy policy must be accessible either in the service contract or on wireless devices, or both, or available elsewhere, such as on a Web site.²¹² The principles also state that the WLIA member must highlight portions of a service contract indicating that the consumer agrees to be located when he or she activates specific location-based features or services.²¹³

²⁰⁹ See WIRELESS LOCATION INDUSTRY ASS’N, ADOPTED WLIA PRIVACY POLICY (FIRST REVISION) (2001), <http://www.wliaonline.org/indstandard/privacypolicy.pdf>.

²¹⁰ *Id.* at 3.

²¹¹ *Id.* at 5.

²¹² *Id.*

²¹³ *Id.* at 6.

²¹⁴ *Id.* at 4. “Confirmed opt-in” is defined as 1) verifying a subscriber’s permission each time the service is provided either through separate contact at that time, or 2) through a process of confirmation that permission has been expressly granted for a period of specific and limited duration made clearly known to the subscriber at the time the subscriber granted permission. Such permission by the subscriber may be expressed at the time of location service activation, customer sign-up, or by other direct communications between the customer and the WLIA member company. It may be expressed by means of writing, electronic communication, voice, or any other means that can be retained in a manner to allow later confirmation that permission was effectively and intentionally granted. *Id.* at 3.

²¹⁵ *Id.* at 8.

its members in order to ensure that the disclosures are sufficiently prominent and understandable to consumers.

²¹⁶ Discussion with John Jimison, Executive Director, WLIA (Aug. 21, 2001).

²¹⁷ This same basic principle governs disclosures made in the course of both online and offline transactions. See FEDERAL TRADE COMM'N, DOT COM DISCLOSURES: INFORMATION ABOUT ONLINE ADVERTISING 4-5 (2000), available at <http://www.ftc.gov/bcp/online/pubs/buspubs/dotcom/index.html>; see also Transcript, *Get Noticed: Effective Financial Privacy Notices*, December 4, 2001, at 162-68, available at <http://www.ftc.gov/bcp/workshops/glb/index.html>.

The wireless devices and services discussed at the workshop are exciting new products and services for consumers. The FTC will continue to monitor their development, along with the privacy, security, advertising, and other consumer protection issues they raise.

Appendix A: List of Workshop Participants

Michael F. Altschul
Vice President/General Counsel
Cellular Telecommunications Industry Association

Michael Amarosa
Vice President Public Affairs
True Position, Inc.

Joseph Assenzo
General Attorney
Sprint PCS

Michael D. Donahue
Executive Vice President
American Association of Advertising Agencies

Janelle W. Edgar
Director of Business Development - Financial and Government
Diversinet

Sean Harrison
President and CEO
WindWire

Evan Hendricks
Editor
Privacy Times

Adonis Hoffman
Senior Vice President and Counsel
American Association of Advertising Agencies

Arthur D. Hurtado
CEO

Robert E. Lewin
President & CEO
TRUSTe

Steven Lucas
Chief Information Officer/Chief Privacy Officer
Persona, Inc.

Mark MacCarthy
Senior Vice President, Public Policy
Visa U.S.A., Inc.

John P. McArtney
Director of Messaging
Verizon Wireless

Amanda McCarthy
Analyst, Telecommunications Group
Forrester Research, Inc.

Shekar Rao
Director - Product Management
Aether Systems, Inc. - Software Product Division

Gregory Miller
Vice President Corporate Development & Chief Privacy Officer
MEconomy, Inc.

David J. Moore
Chief Executive Officer
24/7 Media, Inc.

Walter Mossberg
Personal Technology Columnist
The Wall Street Journal

Jonas Neihardt
Vice-President, Federal Government Affairs
QUALCOMM, Inc.

Jason Pavona
Director of Wireless Strategy and Personalization
Terra Lycos

Barry Peters
Director, Emerging Media
Lot21, Inc.

John Pollard
Director, Business Travel and Mobile Services
Expedia.com

Lawrence A. Ponemon
President
Guardent, Inc.

Richard Purcell
Director, Corporate Privacy Group
Microsoft Corporation

Alan Reiter
President
Wireless Internet and Mobile Computing

Margot Saunders
Attorney
National Consumer Law Center

James D. Schlichting
Deputy Bureau Chief, Wireless Telecommunications Bureau
Federal Communications Commission

Richard Smith
Chief Technology Officer
Privacy Foundation

David L. Sobel
General Counsel
Electronic Privacy Information Center

David Stampley
Assistant Attorney General
Office of the New York Attorney General, Internet Bureau

Steve Stutman
Chief Executive Officer
ClickaDeal.com

FEDERAL