Staff Report

# Public Workshop:

# The Mobile Wireless Web, Data Services and Beyond:

# Emerging Technologies and Consumer Issues

Federal Trade Commission
February 2002

# Contents

# 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.

On the second day of the workshop, panelists discussed the consumer protection issues that wireless technologies raise.[6] Participants explained location-generating technologies that will soon collect precise information about consumers' physical locations as they use their wireless devices and discussed the implications for privacy and security.[7] Then, participants discussed ways to build privacy and security solutions into the technological architecture,[8] as well as other issues raised by advertising on wireless devices.[9] Finally, representatives of self-regulatory groups discussed their programs.[10] After the workshop, the FTC invited written submissions about the issues from interested parties.[11]

This report will address each of the five main topic areas covered in the panels and presentations.

# II. Overview of Wireless Technology

This section summarizes the discussions at the workshop about the wireless Internet and data technologies in use or under development, including location-based services. It also summarizes discussions about some of the challenges and opportunities that the wireless industry faces in the U.S. market.

## A. Background on Wireless Internet and Data Technologies

The wireless Internet is a radio frequency-based service that provides access to the wireless Web and Internet email.[12] The wireless Web includes proprietary Web sites operated by common carriers, sites operated by third parties that have contractual relationships with the carriers, and additional sites formatted for wireless devices.[13] A consumer who owns a Web-enabled mobile phone with the necessary service plan can access the wireless Web by opening the phone's browser and then choosing content from a menu that typically includes messaging

---

6 *Id.*, December 12, 2000, at 186-239. In addition, a representative from the Federal Communications Commission ("FCC") provided an overview of selected rules and statutes governing wireless carriers. *Id.* at 240-49.

7 *Id.* at 251-320.

8 *Id.* at 321-69.

9 *Id.* at 398-454.

10 *Id.* at 372-97.

11 The FTC received one written submission, which is available online at http://www.ftc.gov/bcp/workshops/wireless/comments/index.html.

12 CELLULAR TELECOMMUNICATIONS AND INTERNET ASS'N, THE WIRELESS GLOSSARY, http://www.wow-com.com/consumer/faq/articles.cfm?ID= 98. This Web page is a glossary of terms related to wireless technologies compiled by the Cellular Telecommunications and Internet Association.

13 *See* Pavona, Terra Lycos, at 76; Harrison, Windwire, at 441-42.

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.[21] More recently, manufacturers have introduced hybrid devices that have small screens and offer a variety of features.[22]

---

[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.

contacted at all.[40] The user can also indicate specific interests.[41] The workshop participant stated that Invertix's gateway provides secure links to wireless carriers, secure links to customers, and physical security at its data center.[42]

Wireless carriers are currently working to upgrade the U.S. wireless communication system in order to implement auto-location technology across the country. In October 2001, a handset manufacturer sold the first mobile phones equipped with GPS capabilities, although the auto-location technology does not function yet in most areas of the U.S. because few networks have been upgraded for the service.[43] A carrier launched network-based auto-location technology in limited areas in the U.S. in December 2001.[44] Carriers are continuing to work with software and equipment vendors to implement the services more widely.[45]

## C. Challenges for the Wireless Industry

Workshop panelists discussed the many challenges currently facing the wireless industry, especially in the United States. One major challenge is to create successful business models that engender strong consumer relationships. Many panelists predicted that advertisers will offer discounted or free services in exchange for consumers accepting advertising.[46] Panelists also stated that consumers will be willing to pay for certain applications, such as safety features, customized delivery of information, and messaging capabilities.[47]

A related industry challenge is to increase the adoption of wireless services in the United States. Several panelists noted that European and Japanese consumers have adopted wireless technologies far more quickly than American consumers have.[48] Panelists suggested that numerous factors contribute to the discrepancy in adoption rates. First, Europe and Japan have

---

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 - QUARTERLY REPORT, 1 (February 1, 2002), *at* http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6513075825.

45 *See id.*

46 Cerasale, The Direct Marketing Association, at 111; *see also* McArtney, Verizon Wireless, at 106-7.

47 McCarthy, Visa U.S.A., Inc., at 115; *see also* Carlyle, XY Point Corporation, at 114.

48 Mossberg, The Wall Street Journal, at 20; Pavona, Terra Lycos, at 75-77.

adopted a single technology standard for wireless communications, while the U.S. has not.[49] In Europe and Japan, all cellular devices communicate over the same network, while in the U.S., carriers operate several different networks with competing technologies.[50] Therefore, if a manufacturer wants to introduce a wireless device or service in the U.S. market, it has to design a product or service for each system, and negotiate with each carrier individually, before it can do so.[51] Moreover, three times as many cell towers have to be built in the U.S. because of the three different standards.[52] Second, the U.S. has a much better landline infrastructure than Europe and Japan do, so U.S. consumers have ready access to inexpensive landline telephone calls and to the wired Internet, while many European and Japanese consumers do not.[53] Moreover, in the U.S., cell phone users must pay for every call initiated and received, while in Europe, users only pay for calls they initiate.[54]

Participants stated that consumers are also concerned about poor coverage and the slow speed of wireless connections.[55] Finally, participants noted that it is difficult to enter information into most wireless devices because of small keypads and inaccurate handwriting recognition technology.[56] In order to mitigate this problem, companies are developing technologies such as e-wallets. E-wallets enable consumers to store detailed personal information, including a credit card number, and then later make purchases over the mobile device without re-entering the information every time.[57] Another option that addresses this problem is billing consumer transactions directly to a consumer's mobile phone bill, rather than to a credit card, which is already common in Europe and Japan.[58]

---

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 Pavona, Terra Lycos, at 75.

54 *Id.* at 76.

55 Lawrence, Hewlett-Packard Company, at 153; *see* Mossberg, The Wall Street Journal, at 17. Recently, in January 2002, one carrier launched the first "third generation" or "3G" wireless telephone network in certain regions of the U.S. The 3G network allows faster connection speeds and additional functions, including the ability to send documents, view graphics, download music, and conduct video-conferences through a specially equipped wireless phone or laptop computer. *Verizon Launches First U.S. '3G' Network,* CNN.COM, January 28, 2002, at http://www.cnn.com/2002/TECH/ptech/01/28/verizon.3g/index.html.

56 *See* Mossberg, The Wall Street Journal, at 16.

57 MacCarthy, Visa U.S.A., Inc., at 108-09.

58 *See* Pavona, Terra Lycos, at 88.

# III. Privacy Issues

There was widespread agreement among workshop participants that emerging wireless technologies raise not only many of the privacy issues encountered in the wired world, but new privacy issues as well.[59] This section will discuss the privacy concerns raised by wireless technologies and some possible ways to address them.

## A. Privacy Concerns

Panelists listed the following as the most important privacy concerns related to wireless technologies: collection of location information, tracking visits to wireless Web sites, and increased personal data collection.

### 1. Collection of Location Information

Panelists generally agreed that the generation and potential use of location-based information is one of the most significant privacy issues in the wireless space.[60] Many panelists, representing both industry and consumer groups, stated that location-based services raise concerns because the consumer's specific location can be tracked whenever the user's device is on, which could be a significant portion of the day.[61] Panelists recognized that personally identifiable location information is extremely sensitive.[62] A representative of the Center for Democracy and Technology stated that companies will be able to track location in a way that was never available before, and many consumers do not know about this technology.[63] A privacy and security consultant stated that the collection of detailed location information provides opportunities for abuse of the information.[64] In addition, an industry representative stated that even if the consumer consents to a specific service provider obtaining the location information, once the service provider has the information, others could obtain the data through a court order.[65] Another industry representative expressed concern that certain

---

59 Davidson, Center for Democracy and Technology, at 189. *See also* Ponemon, Guardent, Inc., at 191; Hoffman, American Association of Advertising Agencies, at 147; Hendricks, Privacy Times, at 304; Donahue, American Association of Advertising Agencies, at 408.

60 Davidson, Center for Democracy and Technology, at 190; Ponemon, Guardent, Inc., at 192-93; *see* Moore, 24/7 Media, Inc., at 196.

61 Hendricks, Privacy Times, at 294; *see also* Cranor, AT&T Labs-Research, at 195; Weisler, Vindigo Company, at 296.

62 *See* Ponemon, Guardent, Inc., at 192-93, Davidson, Center for Democracy and Technology, at 207.

63 Davidson, Center for Democracy and Technology, at 190.

64 Bromley, Fiderus Strategic Security and Privacy Services, at 194.

65 Cranor, AT&T Labs-Research, at 196.

companies may consider a consumer's location and location history to be information that should be available to any entity possessing the technology to capture it.[66]

According to workshop participants, a typical cell phone that is turned on sends out signals every ten minutes and identifies the location of the nearest cell tower.[67] In less populated areas, cell towers are located about every thirty miles, but in cities, cell towers are located about every two blocks.[68] These signals can be used to determine a cell phone user's location, so that even without the precise auto-location technologies discussed above (e.g., GPS), a user's location can be pinpointed fairly precisely in some areas.[69] For the most part, carriers are not currently archiving this location information; however, companies may develop new business models to archive and use such information in the near future.[70] Moreover, GPS and the other auto-location technologies will soon generate location data that identifies the user's precise location at any given moment when the device is turned on.

As discussed at the workshop, the FCC has issued a set of rules, called the Enhanced 911 ("E911") rules, that require wireless carriers to collect precise location information in the near future in order to improve the delivery of emergency services. Today, although a 911 operator receives exact information about a caller's location upon receiving a landline call, that is not the case with all cellular calls to 911.[71] For many cellular calls, the operator has to ask for the caller's location first, slowing down the needed emergency services.[72] The problem is exacerbated when the caller does not know where he or she is, and thus the dialogue can take a significant amount of time.[73]

The FCC's E911 rules require common carriers to adapt their wireless networks so that they automatically provide certain information to 911 call centers.[74] The initial rules, which have already been implemented in some areas, require wireless carriers to provide the caller's telephone number and generalized location information – typically the location of the cellular tower nearest to the caller – to the call center when a consumer dials 911. The rules then require carriers to begin implementing precise auto-location technology for transmission to 911

---

66 Carlyle, XY Point Corporation, at 297.

67 Cranor, AT&T Labs-Research, at 195.

68 *Id.*

69 *Id.*

70 *Id.*

71 Schlichting, FCC, at 242.

72 *Id.*

73 *Id.*

74 *Id.* For additional details about the FCC's Enhanced 911 rules, see http://www.fcc.gov/e911/.

call centers.[75] Once these procedures are fully implemented, 911 operators will be able to identify a cellular caller's precise location immediately upon picking up the call.

An industry representative stated that, because carriers are required to collect precise location information for emergency purposes, it is likely that businesses will find commercial applications for the information once collected.[76] To address privacy concerns arising from these potential commercial uses, a provision of the Wireless Communications and Public Safety Act of 1999 amended the Telecommunications Act to provide that carriers must obtain "express prior authorization" before releasing this location information to third parties.[77] The FCC has not yet begun a rulemaking to provide further guidance on implementing this statutory provision.[78]

The Wireless Communications and Public Safety Act of 1999 also provides that information collected about a consumer's location is to be treated as customer proprietary network information ("CPNI"), which is data about a customer's telephone service and usage that receives special legal protections under Section 222(c)(1) of the Telecommunications Act of 1996.[79] The 1996 statute provides that carriers must obtain "the approval of the customer" before sharing CPNI with a third party (unless a specific statutory exception applies).[80] In 1998, the FCC issued an implementing regulation that defined "approval of the customer" as opt-in consent from the customer.[81] Subsequently, the Tenth Circuit vacated the rule's opt-in

---

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), http://www.fcc.gov/Bureaus/Wireless/News_Releases/2001/nrwl0127.html. The major wireless carriers filed quarterly status reports with the FCC detailing the status of the rollout of auto-location technology on or around February 1, 2002. These reports are available by searching Docket Number 94-102 in the FCC's Electronic Comment Filing System, http://www.fcc.gov/e-file/ecfs.html.

76 *See* Carlyle, XY Point Corporation, at 289.

77 Schlichting, FCC, at 246; 47 U.S.C. § 222(f) (Matthew Bender & Company, LEXIS through Nov. 6, 2001).

78 In November 2000, the Cellular Telecommunications and Internet Association ("CTIA") filed a petition with the FCC requesting such a rulemaking and asking that the FCC adopt the CTIA's proposed privacy guidelines as a safe harbor for any location information service provider that follows the principles. In March 2001, the FCC issued a notice requesting comments to help determine whether it should proceed with the rulemaking that the CTIA requested. About fifty entities filed comments on the petition, and the comment period closed on April 24, 2001. To date, the FCC has not issued a decision on the petition.

79 47 U.S.C. § 222.

80 47 U.S.C. § 222(c)(1).

81 Second Report and Order, 63 Fed. Reg. 20326, 20329 (1998) (to be codified at 47 C.F.R. pt. 64); Schlichting, FCC, at 246.

requirement because of First Amendment concerns.[82] In October 2001, the FCC issued a notice seeking comment as to whether the FCC could meet the constitutional test and therefore should adopt opt-in consent, or should instead adopt opt-out consent for the carriers' use of CPNI under Section 222(c)(1).[83] In addition, recognizing that two subsections of the Telecommunications Act regulate location information using different language ("express prior authorization" versus "approval of the customer"), the notice sought comment on what effect, if any, the provisions of section 222(f) have on the FCC's interpretation of section 222(c)(1).[84] The FCC is currently reviewing the comments that it received and has not yet issued a final rule.

Even in the absence of final regulations interpreting these provisions, the statutory language itself clearly provides certain protections for location information and CPNI – namely, that in most situations carriers obtain some form of consent before disclosing a consumer's phone records to a third party.[85] One panelist noted that even these protections are limited, however, because they impose restrictions on common carriers but place no limitations on re-disclosure by third parties, such as wireless content providers, that receive the location information from common carriers.[86]

### 2. Tracking Visits to Wireless Web Sites

Panelists stated that, as with surfing the wired Internet, users' browsing patterns on the wireless Web may be monitored and traced to individuals.[87] As an individual surfs the mobile Web, the carrier and third-party content providers can collect a unique identifier, and possibly even the consumer's mobile phone number.[88] Panelists pointed out that a person's wireless device tends to be strongly tied to an individual, even more so than a computer typically is, because people are less likely to share a wireless device with others; therefore, the potential

---

82 *U.S. West, Inc. v. FCC,* 182 F.3d 1224, 1240 (10th Cir. 1999). The court stated that because customer phone records are protected commercial speech, the government must 1) "specifically articulate and properly justify" that the regulation's goal constitutes a substantial state interest; 2) show that the regulation directly and materially advances that interest; and 3) show that the regulation is no more extensive than necessary to serve the interest. *Id.* at 1233. The court found that the FCC had failed to meet this burden because 1) the FCC asserted a broad interest in privacy but did not specify the particular notion of privacy and interest served; 2) the FCC did not present evidence showing the harm to privacy was real; and 3) the FCC record did not adequately show that an opt-out strategy would not sufficiently protect customer privacy. *Id.* at 1234-39.

83 Proposed Rule, 66 Fed. Reg. 50140, 50140 (2001). *See also* Schlichting, FCC, at 246; 47 U.S.C. § 222(c).

84 66 Fed. Reg. at 50142.

85 *See* 66 Fed. Reg. at 50141.

86 *See* Hendricks, Privacy Times, at 294-95.

87 Davidson, Center for Democracy and Technology, at 190-91.

88 *Id.*

consequences of an individual being tracked on the wireless Web are more significant than if the user were being tracked on the wired Internet.[89]

A representative of a wireless content provider recognized that even companies that are not subject to FCC regulations (such as content providers, which are not common carriers under the statute) want to build trust with consumers, and they can do so by keeping consumers anonymous instead of tracking them on an identifiable basis.[90] A representative of Sprint PCS stated that Sprint encrypts the user's telephone number when the user is surfing the wireless Web so that the user can remain anonymous.[91] A consumer advocate urged companies not to use consumers' unique identifiers if they do not need to do so.[92] Another panelist stated that numerous parties, including content providers and software developers, will need to work together to make sure that the user's phone number or a unique identification number will not be broadcast to every wireless Web site a consumer visits.[93]

### 3. Greater Personal Data Collection

Panelists stated that wireless content is frequently most valuable to consumers when it is personalized.[94] Therefore, businesses may seek to collect large amounts of highly personal information for use in personalization.[95] Panelists predicted that wireless advertising, in particular, will be highly targeted and will focus on customer retention and customer relationship management instead of focusing on recruiting new customers.[96] Panelists recognized, however, that collecting large amounts of highly personal information provides opportunities for abuse by the companies collecting it.[97] In addition, law enforcement agencies may seek access to such information in criminal investigations,[98] and civil litigants may seek

---

89 *Id.* at 191; Lucas, Persona, Inc., at 418.

90 Weisler, Vindigo Company, at 310.

91 Assenzo, Sprint PCS, at 312-13.

92 Hendricks, Privacy Times, at 304.

93 Cranor, AT&T Labs-Research, at 212.

94 For example, a consumer who likes coffee might be happy to receive a cellular phone call offering a discount on a cup of coffee at a shop around the corner from where the consumer is located at that particular moment. Ponemon, Guardent, Inc., at 192.

95 *Id.* at 191; Bromley, Fiderus Strategic Security and Privacy Services, at 194; Hendricks, Privacy Times, at 295.

96 Donahue, American Association of Advertising Agencies, at 419; Peters, Lot21, Inc., at 407.

97 Bromley, Fiderus Strategic Security and Privacy Services, at 194; *see* Hendricks, Privacy Times, at 295.

98 Davidson, Center for Democracy and Technology, at 206; Cranor, AT&T Labs-Research, at 223.

access to the same information through civil process.[99] Thus, some panelists suggested that companies should not collect information that they do not need, such as Social Security numbers.[100]

## B. Addressing Privacy Concerns in the Wireless Space

Participants provided numerous suggestions to address privacy concerns in the wireless space. This section will discuss recommended privacy protections and ways to build privacy into the technological architecture.

### 1. Privacy Protections for Wireless Services

Many workshop participants agreed that the intrusive and costly nature of offers and solicitations in the wireless space warrant special protections.[101] A representative of the Center for Democracy and Technology stated that the information that wireless devices can collect is extremely sensitive.[102] One panelist noted that it would be very problematic if a consumer gets unwanted solicitations on a wireless device or if the information gets into the wrong hands.[103] Another panelist stated that consumers want privacy protections for information collected through wireless devices.[104] Therefore, many workshop participants agreed that consumers should be given some form of control over information collected and used in the wireless space.[105]

Panelists pointed out, however, that providing effective notice about information practices will be challenging, in a practical sense, because the screens on most wireless devices are so small that privacy policies are difficult to read.[106] Many cellular phones only allow eighteen

---

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; Moore, 24/7 Media, Inc., at 200; Bromley, Fiderus Strategic Security and Privacy Services, at 202; Harrison, Windwire, at 413; Donahue, American Association of Advertising Agencies, at 419.

106 Ponemon, Guardent, Inc., at 198; Lewin, TRUSTe, at 424.

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 should be clear, robust, and easy to understand.[114] Another panelist stated that posting long privacy disclosures on wireless Web sites would likely be obtrusive.[115] He therefore suggested that businesses consider posting short versions of their policies on their wireless Web sites, and making a more comprehensive disclosure available on a wired Web site or through an 800 number – as long as these alternatives are made clear to the consumer using the wireless device.[116] Panelists also recognized that many wireless transactions, such as viewing a bank account balance, will take place after the consumer

---

[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 panelists acknowledged that some companies will nevertheless send such messages.[119] A representative from a wireless advertising technology company stated that advertisers should get opt-in consent before sending "push" advertising (where advertising content is sent to a wireless device at a time other than when the user requests it).[120] However, he did not support opt-in consent for "pull" advertising (where the user goes to a Web site to receive information and receives an advertisement with the information), because it would be annoying to the consumer to have to agree to each advertisement that is served with requested content.[121]

Regarding advertising and tracking of wireless Web users' surfing habits, one panelist suggested that users should be given two options when they first sign a contract for wireless service: 1) to pay for the content without any advertising, or 2) to get free content by agreeing to accept advertising and allow advertisers to track their Web site surfing and purchases, so that advertisers can profit from the advertising.[122]

Many panelists supported added protections when location information is at issue.[123] One consumer advocate stated that any consent to disclose location information must be truly informed consent, in order to give consumers confidence in the medium.[124] He advised companies to set the default on wireless devices and systems so that there is no tracking of the consumer's location. Thus, consumers would have to activate the devices to enable location tracking (although the default should be overridden for 911 calls, so that people can be located

---

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.

that govern wireline communications.[142] Other vulnerabilities exist once the transmission arrives at the wired Internet and becomes subject to the security vulnerabilities of the wired Internet.[143]

Wireless devices are also easy to misplace and relatively easy to steal. As wireless devices become capable of storing more information, and conducting more sophisticated information processing, consumers have more information at stake if they lose their devices.[144] Consumers already store highly sensitive information in their wireless devices – for example, many doctors store detailed patient information in their handheld devices.[145] Thus, losing the device could compromise highly sensitive information and increase the risk of identity theft to the owner and others.[146]

Panelists suggested that strong authentication procedures should be in place to prevent security breaches.[147] They pointed out that such security systems should be transparent and intuitive to users.[148] Currently, many cellular phones are enabled with locks to prevent unauthorized access to them, but most consumers do not routinely use the lock function because it is not convenient.[149] Advances in technology could allow the owner to lock the device from a remote location if it is lost, even if the user did not lock the device beforehand.[150] Security features also need to be affordable, and some security features may be so expensive that adding them would dissuade people from buying wireless products.[151]

In addition, a representative of the technology infrastructure company MEconomy, Inc. made several recommendations to improve wireless security, including 1) using an open platform for devices so users can load and unload their own privacy and security technologies; 2) separating personal identifiers from transactional data to increase privacy and security; and

---

[142] *Id.* at 215. Since the two systems are different, transactions must be decrypted in one system and then re-encrypted before being transmitted to the other system. The content is insecure for a short period of time, and a hacker could target the data at that time. *See id.*

[143] *Id.* at 216.

[144] *Id.*; *see* Lucas, Persona, Inc., at 439.

[145] Ponemon, Guardent, Inc., at 193.

[146] Bromley, Fiderus Strategic Security and Privacy Services, at 216.

[147] *Id.*

[148] Smith, Privacy Foundation, at 343; *see* Purcell, Microsoft Corporation, at 335.

[149] Purcell, Microsoft Corporation, at 343-44.

[150] Ponemon, Guardent, Inc., at 193.

[151] Miller, MEconomy, Inc., at 344.

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 infrastructure[153] 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;[156] thus, there would be no legal requirement that the seller provide a mechanism for dispute resolution if the consumer alleges that unauthorized charges were made through the device.[157] The panelist recommended that if possible, consumers should use their credit cards to engage in m-commerce transactions.[158]

# V. Advertising and Disclosures

## A. What Forms Advertising Will Take

Panelists at the workshop stated that advertising firms are already delivering advertisements to cellular phones and PDAs.[159] They have found, however, that serving advertisements on mobile devices is challenging because the screens are small, and it is difficult to serve advertisements across different devices and multiple carriers.[160] Panelists also noted that wireless advertisements can be text-only, voice-based, or a combination of text and voice.[161] For example, "call-through" technology, discussed above, allows a consumer to click on a text-based hyperlink, which then automatically calls the advertiser so that the consumer can talk on the phone with the advertiser or listen to a recorded message.[162] Several panelists

---

[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.[165] On PDAs, advertisers can serve interstitial advertisements, which are full-page advertising messages that appear for a few seconds between a user's current and destination pages.[166] Advertisers can also place text-based advertisements in the top section of the PDA screen, a format that is similar to placing a banner advertisement in the wired space.[167]

## B. Advertising Disclosures

Certain advertising claims require that the advertiser make additional disclosures to consumers about the terms and conditions of the promotions in order to prevent deception.[168] Panelists raised many of the same issues with respect to advertising disclosures that were discussed in connection with privacy disclosures – namely, that it is difficult to ensure that the disclosures are visible and understandable on the small screens of wireless devices.[169]

A representative of a wireless advertising company made the following suggestions: 1) place the disclosure beneath the advertisement and allow the user to scroll down and obtain additional information; 2) provide information at the bottom of the screen in the link section; or 3) for cellular phones, enable the user to call through to a call center or a recording where the user can listen to the full disclosure of terms and conditions.[170] Another panelist stated that because many wireless transactions will occur after a consumer has signed up for a specific wireless service on the wired Internet, the appropriate disclosures can be presented on a wired Web page.[171] Finally, one panelist recognized that advertisements for certain products, such as

---

[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.

prescription medications, may not be appropriate for wireless devices at all because the necessary disclosures are so lengthy.[172]

A representative of the National Consumer Law Center stated that the Electronic Signatures in Global and National Commerce Act ("E-SIGN")[173] and other laws may allow consumers to engage in more transactions over the Internet.[174] She stated that it is important that a consumer be able to retain a record of the material terms of the transaction; however, in the wireless space, there is no direct mechanism for saving or printing important documents, such as those terms and conditions.[175] The panelist recognized that this concern may be alleviated if consumers use credit cards for purchases, because credit cards provide special legal protections.[176] Moreover, another panelist stated that, where the consumer purchases a product over a wireless device, a manufacturer could send a written copy of the terms and conditions with the product to further address these concerns.[177]

## VI. Self-Regulatory Programs

At the workshop, panelists described three self-regulatory programs being developed to address some of the privacy, security, and advertising issues raised at the workshop. The organizations that are developing these programs are: the Cellular Telecommunications and Internet Association ("CTIA"), the Wireless Advertising Association ("WAA"),[178] and the Wireless Location Industry Association ("WLIA"). The FTC staff supports self-regulation in the wireless area and encourages further development of these programs, which are described below.

---

172 Harrison, Windwire, at 430-31.

173 15 U.S.C. § 7001 (Matthew Bender & Company, LEXIS through Nov. 6, 2001).

174 Saunders, National Consumer Law Center, at 151-52. Congress enacted E-SIGN to facilitate the use of electronic records and signatures in interstate or foreign commerce. E-SIGN was intended to eliminate barriers to electronic commerce but also provide consumers with protections, including those equivalent to paper-based transactions.

175 *Id.*

176 *Id.* at 163-64. In addition, Section 101(e) of E-SIGN states that if a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be in writing, the legal effect, validity, or enforceability of an electronic record of such contract or other record may be denied if such electronic record is not in a form that is capable of being retained and accurately reproduced for later reference by all parties or persons who are entitled to retain the contract or other record. 15 U.S.C. § 7001(e).

177 Hyer, AT&T Wireless Services, Inc., at 154.

178 On January 10, 2002, the WAA announced that as of January 28, 2002, it would be merging with the Wireless Marketing Association to create the Mobile Marketing Association ("MMA").

## 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.*

## B. Wireless Advertising Association/Mobile Marketing Association

The WAA/MMA member companies are manufacturers, advertising networks, advertising agencies, wireless application service providers, publishers, and wireless advertising service providers.[193] At the workshop, a representative stated that the organization (then called the Wireless Advertising Association) had developed privacy guidelines to which its members must adhere in order to put consumers in control of their personally identifiable information (PII) and to promote a climate of trust between consumers and the industry.[194]

The WAA/MMA guidelines define PII as data that can be used to identify or contact a person uniquely and reliably.[195] Thus, a static unique identifier, even if it is not connected to an individual's name, would be considered PII under the guidelines.[196] However, the guidelines do not clarify whether location information would or would not be considered PII.[197]

The guidelines require members to notify subscribers of how PII is being used, provide choice regarding the use of PII, make every effort to ensure that PII is accurate and secure, and where reasonable and appropriate, allow subscribers to correct or delete such information.[198] The guidelines require that privacy policies should be easy to find, read, and understand.[199] In addition, before sending any "push" messaging,[200] and before using PII for any reason other than that for which it was initially gathered, the guidelines specify that members must use "confirmed opt-in" choice.[201] "Confirmed opt-in" is defined as a process of

---

193 DePriest, WAA, at 378.

194 *Id.* at 379. The American members of the newly created MMA plan to adhere to the principles that the WAA developed. The organization has not yet determined whether European companies in the organization will be required to sign on to the principles, given that those companies are likely already complying with privacy laws. Telephone Interview with John Kamp, Counsel, WAA (January 11, 2002).

195 WAA/MMA GUIDELINES § II(A).

196 Telephone Interview with John Kamp, Counsel, WAA (November 15, 2001).

197 Location information that is tied to an identifier would logically fall within the guidelines' definition of PII. *See* WAA/MMA GUIDELINES § II(A). However, the guidelines appear to classify location information as non-PII by stating that "the WAA intends to address notification and consent issues related to non-PII, *including location-based advertising and or content*, in a future version of the guidelines." *Id.* at § I (emphasis added). To date, the organization has not issued any additional guidelines.

198 DePriest, WAA, at 381-82.

199 WAA/MMA GUIDELINES § IV.

200 As noted above, "push" messaging is defined as advertising content that is sent to a wireless device at a time other than when the subscriber requests it.

201 WAA/MMA GUIDELINES § 5(A). A Direct Marketing Association representative questioned whether this guideline was workable, because a marketer sending a communication to an email address would not know whether the recipient will view the communication on a personal computer or a wireless device. Thus, the marketer would have to comply with the guidelines for wireless devices every time it sent out any

verifying a subscriber's permission in order to ensure that content is not accidentally or maliciously sent to the subscriber's wireless mobile device.[202] For example, after receiving permission from a subscriber, an advertiser or marketer may send a follow-up message to the subscriber to which he or she must positively reply in order to confirm permission to start receiving messages.[203]

Thus, the guidelines require that notice relating to PII be clear and easy to find, and provide a consent mechanism to ensure that consumers do not receive messages they do not want. In a recent meeting with FTC staff, WAA representatives affirmed the importance of clear and conspicuous disclosures, stating that they do not want consumers to be confused, as consumer confusion would slow adoption of the services.[204] However, to assist member companies in complying with the guidelines, FTC staff suggested that the organization provide additional guidance regarding the content and placement of these privacy disclosures.[205] The FTC staff also urges the WAA/MMA to clarify whether consumers' location data would or would not be considered to be PII under the guidelines.[206]

## C. Wireless Location Industry Association

The WLIA is a new organization whose member companies provide hardware, software, services, and other products related to the identification of the precise location of wireless users. In November 2000, these companies decided that the issues they faced were unique and formed their own organization.[207] At the workshop, the WLIA stated its intention to set high standards for its members, and to reward companies that meet those standards and sanction companies that do not.[208]

---

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

202 WAA/MMA GUIDELINES § II(F).

203 *Id.*

204 Discussion with John Kamp, Marci Weisler, and Barry Peters, WAA representatives (Oct. 14, 2001).

205 *Id.*

206 Following the presentations by the CTIA and WAA, a representative of EPIC, a public interest research center, commented on the guidelines. He stated that there seemed to be a developing consensus on many of the points that are important to most users and consumers, including that 1) consumers should be well informed of the collection and use practices of the provider; 2) businesses should provide a meaningful opportunity to consumers to provide their consent; and 3) uniform guidelines should be established that focus on the type of information being collected and establish consumer rights. However, he stated that legislation may be necessary in order to further encourage self-regulation, to ensure uniformity, and to address issues such as legal access in criminal investigations and civil litigation. Sobel, Electronic Privacy and Information Center, at 386-92.

207 Jimison, WLIA, at 383-84.

208 *Id.* at 385-86.

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]

In addition, the standards require WLIA members to use personally identifiable location data solely for the purposes for which it was obtained, and not for any other purposes without "confirmed opt-in" permission. The WLIA definition of "confirmed opt-in" differs from the WAA/MMA definition in that "confirmation" may consist of a separate contact to verify permission (like the WAA/MMA guidelines) or retention of a record of the consumer's explicit agreement to the information use.[214] A member that is adjudged to have violated the WLIA standards or its own privacy policy (pursuant to a procedure set forth in the WLIA policy) may lose WLIA member privileges, be expelled from the WLIA, be referred by the WLIA to appropriate regulatory authorities, or be subject to other sanctions.[215]

The WLIA guidelines thus include requirements designed to ensure clear and conspicuous disclosures about the use of consumers' location information, as well as an opt-in requirement for uses of the data other than those for which the information was obtained. In discussions with the WLIA, the FTC staff again suggested that the WLIA provide continuing guidance to

---

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]

## VII. Conclusion

The purpose of this workshop was to educate Commission staff and the public about new mobile wireless technologies and to explore the consumer protection issues that they raise. The presentations and panel discussions encouraged a dialogue that was educational and useful, and identified issues that warrant continuing attention as wireless technologies develop.

Participants generally agreed that privacy, security, and advertising issues are significant concerns in the wireless environment. In particular, they noted that the intrusive and costly nature of wireless offers raises unique privacy and security issues, and that it is difficult to make effective disclosures in the wireless context. In addition, they discussed the special privacy and security issues raised by the collection of detailed data about a consumer's physical location. Many workshop participants therefore agreed that consumers should be given some form of control over information collected and used in the wireless space, particularly when location information is at issue.

Several self-regulatory groups have already proposed or established guidelines that address some of the concerns raised at the workshop. Although they apply to different entities and contain certain differences, all of them call for some form of notice and opt-in choice applicable to personally identifiable information and/or location information in the wireless space. The FTC staff encourages self-regulation in this area and applauds these efforts.

However, as discussed above, the staff believes that more guidance may be helpful to companies seeking to implement these guidelines. In particular, additional guidance could help to ensure that the methods used by companies to provide notice and choice to consumers are clear and conspicuous. To be clear and conspicuous, disclosures should be communicated effectively so that consumers are likely to notice and understand them.[217] Although the guidelines' general standards are, for the most part, consistent with this goal, additional guidance may be needed to ensure that the examples provided in some of the guidelines – *e.g.*, disclosures in a service contract or phone bill and choice provided through a "clickwrap" agreement – are implemented in a clear and conspicuous manner. Further, companies may want such additional guidance as they seek concrete and practical ways to fulfill the guidelines' general standards.

---

[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/conline/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

Eric Bergeron
General Manager - Wireless Solutions
Zero-Knowledge Systems, Inc.

William K. Bodin
Senior Technical Staff Member in Advanced Technology/Research
IBM Pervasive Computing Division

Donald A. Bromley
Practice Leader, Wireless Risk Management Services
Fiderus Strategic Security and Privacy Services

Reuven Carlyle
Vice President, Strategic Planning
XY Point Corporation

Jerry Cerasale
Senior Vice President, Government Affairs
Direct Marketing Association, Inc.

Lorrie Faith Cranor
Senior Technical Staff Member
AT&T Labs - Research

Alan Davidson
Staff Counsel
Center for Democracy and Technology

Timothy DePriest
Chair, Wireless Advertising Association
AdForce Everywhere

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
Invertix Corporation

J. Walter Hyer III
Vice President & Associate General Counsel
AT&T Wireless Services, Inc.

John W. Jimison
General Counsel and Executive Director
Wireless Location Industry Association
Berliner, Candon & Jimison

Peter Lawrence
Business Development Manager
Internet and Wireless Service Organization
Hewlett-Packard

Rick Lane
Director, eCommerce and Technology
U.S. Chamber of Commerce

Mark LeMaitre
Director - Technology Strategy
Nextel Communications, Inc.

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

Marci Weisler
Vice President, Business Development
Vindigo Company

Daniel J. Weitzner
Technology and Society Domain Leader
World Wide Web Consortium