Order Code RL31636

CRS Report for Congress
Received through the CRS Web

Wireless Privacy and Spam: Issues for Congress

Updated January 26, 2005

Marcia S. Smith
Specialist in Aerospace and Telecommunications Policy
Resources, Science, and Industry Division

Wireless Privacy and Spam: Issues for Congress

Summary

Wireless communications devices such as cell phones and personal digital assistants (PDAs) are ubiquitous. Some consumers, already deluged with unwanted commercial messages, or "spam," via computers that access the Internet by traditional wireline connections, are concerned that such unsolicited advertising is expanding to wireless communications, further eroding their privacy.

In particular, federal requirements under the Enhanced 911 (E911) initiative to ensure that mobile telephone users can obtain emergency services as easily as users of wireline telephones, are driving wireless telecommunications carriers to implement technologies that can locate a caller with significant precision. Wireless telecommunications carriers then will have the ability to track a user's location any time a wireless telephone, for example, is activated. Therefore some worry that information on an individual's daily habits — such as eating, working, and shopping — will become a commodity for sale to advertising companies. As consumers walk or drive past restaurants and other businesses, they may receive calls advertising sales or otherwise soliciting their patronage. While some may find this helpful, others may find it a nuisance, particularly if they incur usage charges.

As with the parallel debates over Internet privacy and spam, the wireless privacy discussion focuses on whether industry can be relied upon to self-regulate, or if legislation is needed. Three laws already address wireless privacy and spam concerns. The 1991 Telephone Consumer Protection Act (TCPA, P.L. 102-243) prohibits the use of autodialers or prerecorded voice messages to call wireless devices if the recipient would be charged for the call, unless the recipient has given prior consent. The 1999 Wireless Communications and Public Safety Act (the "911 Act," P.L. 106-81) expanded on privacy protections for Customer Proprietary Network Information (CPNI) held by telecommunications carriers by adding "location" to the definition of CPNI, and set forth circumstances under which that information could be used with or without the customer's express prior consent. The 2003 Controlling the Assault of Non-Solicited Pornography and Marketing Act (the CAN-SPAM Act, P.L. 108-187) required the Federal Communications Commission (FCC) to issue rules to protect wireless subscribers from unwanted mobile service commercial messages (they were issued in August 2004). Consumers also may list their cell phone numbers on the National Do Not Call Registry.

Congress continues to debate how to protect the privacy of wireless subscribers. Representative Frelinghuysen has introduced H.R. 83 in the 109th Congress, which requires wireless telecommunications carriers to adhere to the fair information practices of notice, choice, and security in obtaining the express prior consent required by the 911 Act. Congress also is debating issues associated with an ongoing effort to develop a "wireless 411" telephone directory. The major question is whether a law is needed to ensure that subscribers have the right to decline to have their cell phone numbers listed, at no charge. Representative Pitts has announced his intent to reintroduce legislation that he offered in the 108th Congress on that issue.

This report is updated as warranted.

Contents

Introduction 1

Concerns of Consumers and Privacy Rights Advocates 2
- Spam 2
- "Wireless 411" Directories 3
- Other Concerns 5

Fair Information Practices 5

Industry Efforts to Respond to Privacy Concerns 6

Existing Laws 8
- The Telephone Consumer Protection Act (TCPA) 8
- The Wireless Communications and Public Safety Act (the "911 Act") 8
- The CAN-SPAM Act 10

Legislation in the 109th Congress 12
- Wireless Privacy: H.R. 83 (Frelinghuysen) 12

Appendix: Legislative Action in the 108th Congress 13
- Wireless Privacy: H.R. 71 (Frelinghuysen) 13
- "Wireless 411" Directory Assistance: H.R. 3558 (Pitts), S. 1963 (Specter), and S. 1973 (DeWine) 13

Wireless Privacy and Spam: Issues for Congress

Introduction

Wireless communications devices — including mobile telephones, personal digital assistants (PDAs), pagers, and automobile-based services such as OnStar — are ubiquitous.[1] Many of the services provided by these devices require data on the user's location, whether it is to connect a phone call or dispatch emergency services when an airbag deploys.

Consumers and privacy rights advocates are increasingly concerned about the privacy implications of these wireless location-based services. If a company providing a wireless service knows the user's location, with whom can that data be shared? How long can the data be retained? Will the data be used to create individual profiles that will be sold to marketing companies or used for other purposes unknown to the user or contrary to his or her preference? Will consumers be deluged with messages on their communications devices advertising sales at nearby stores or restaurants not unlike the "spam"[2] in their e-mail inboxes?

The precision with which wireless service providers can determine a subscriber's exact location is improving with the implementation of Enhanced 911 (E911) capabilities for mobile telephones and other wireless devices, wherein wireless carriers are required to provide Public Safety Answering Points (PSAPs) with the location of wireless callers who dial 911 within 50-300 meters (150-900 feet).[3] While this serves the laudable goal of ensuring mobile telephone users immediate access to emergency services, many worry about what other uses will be made of such location information. Once the technical ability exists to provide a user's precise coordinates, some privacy advocates worry that more and more devices will incorporate it, making location information widely available without proper privacy safeguards.

---

[1] The Cellular Telecommunications & Internet Association (CTIA) maintains a counter on its website [http://www.ctia.org] showing the number of U.S. wireless subscribers. On November 1, 2004, the figure was approximately 171 million.

[2] For more information on "spam," see CRS Report RL31953, *"Spam": An Overview of Issues Concerning Commercial Electronic Mail*, by Marcia S. Smith.

[3] For more information on E911, see CRS Report RS21222, *Implementing Wireless Enhanced 911 (E911): Issues for Public Safety Answering Points (PSAPs)*, by Linda K. Moore, and CRS Report RS21028, *Wireless Enhanced 911 (E911): Issues Update*, by Linda K. Moore.

The debate over wireless privacy in many ways parallels the debate over Internet privacy [4] and Internet spam. Indeed, since wireless Internet access devices are on the market, the issues intersect. One particular similarity is that the policy debate focuses on whether legislation is needed, or if industry can be relied upon to self-regulate.

Three laws address some of the issues — the Telephone Consumer Protection Act, the Wireless Communications and Public Safety Act, and the CAN-SPAM Act. Four bills were considered by the 108th Congress that further addressed wireless privacy issues, but none passed. They are described in the appendix to this report. One of the bills has been reintroduced in the 109th Congress, and is discussed below.

Concerns of Consumers and Privacy Rights Advocates

Spam

Some consumers and privacy rights groups, including the Center for Democracy and Technology (CDT) [http://www.cdt.org] and the Electronic Privacy Information Center (EPIC) [http://www.epic.org], worry that the ability to identify a wireless customer's location could lead to further erosion of individual privacy. Although the E911 requirements apply only to calls made from mobile telephones seeking emergency assistance, once that capability is available, many worry that such information will be collected and sold for other purposes, such as marketing. Some observers point out that wireless carriers may be motivated to sell such customer data to recoup the costs of deploying wireless E911.

Users of wireless devices such as pagers, personal digital assistants, or automobile-based services such as OnStar, might be affected along with mobile telephone customers. A major concern is that if location information is available to commercial entities, a wireless customer walking or driving along the street may be deluged with unsolicited advertisements from nearby restaurants or stores alerting them to merchandise available in their establishments. Supporters of unsolicited advertising insist that consumers benefit from directed advertisements because they are more likely to offer products in which the consumer is interested. They also argue that advertising is protected by the First Amendment.

One aspect of this concern is that companies could build profiles of consumers using data collected over a period of time. In that context, one question is whether limits should be set on the length of time location information can be retained. Some argue that once a 911 call has been completed, or after a subscriber to a location-based service received the desired information (such as directions to the nearest restaurant), that the location information should be deleted.

---

[4] For more on Internet privacy, see CRS Report RL31408: *Internet Privacy: Overview and Pending Legislation*, by Marcia S. Smith.

Wireless spam was addressed by Congress in the CAN-SPAM Act (discussed below), although it does not focus specifically on the location aspects of the issue.

"Wireless 411" Directories

Another aspect of the wireless privacy debate concerns the rights of subscribers to have, or not have, their numbers listed in a "wireless 411" cell phone directory. Such a directory does not currently exist, but the Cellular Telecommunications & Internet Association (CTIA) is developing one for six of the seven largest mobile service providers — ALLTEL, Cingular, AT&T Wireless, Nextel, Sprint, and T-Mobile. The seventh, Verizon Wireless, declined to participate, however (discussed below). One estimate is that a wireless directory could generate as much as $3 billion a year for the wireless industry by 2009 in fees and additional minutes.[5] Qsent is the "aggregator" for the directory service.[6]

In early 2005, two of the six companies backing the directory project, Sprint and ALLTEL, announced changes in their plans regarding the directory. According to the trade publication *TR Daily*, a Sprint spokesman stated that Sprint will remain an active participant in creating the directory, but will not offer it in 2005 — the company will reassess its position as the regulatory climate changes, particularly in the states.[7] TR Daily quoted an ALLTEL spokesman saying that his company also decided to wait until the regulatory situation becomes clearer, and that the company is "not likely" to offer the directory in 2005.[8] The ALLTEL spokesman reportedly cited a new California law specifically, which requires carriers to obtain separate authorization from subscribers before including them in the directory, as an example of the evolving regulatory climate.

A key difference between wireless and wireline phones is that subscribers must pay for incoming as well as outgoing calls. Thus, some argue that subscribers need to be assured that they will not receive unwanted calls, not only because of a nuisance factor, but for cost reasons. Consumers may list their cell phone numbers on the National Do Not Call Registry (see CRS Report RL31642), but concerns persist about unwanted calls from telemarketers or others. (In December 2004, an e-mail was widely circulated on the Internet warning consumers that they must list their cell phone numbers on the Do Not Call list before the end of 2004, but that is incorrect. Phone numbers may be added to the Do Not Call list at any time. See [http://www.ftc.gov/donotcall/] for information on the Do Not Call list).

Questions that are arising include whether subscribers should be able to decline to have their numbers published without paying a fee (as wireline customers must do if they want an unlisted number). Proponents of the directory insist that customers

---

[5] Shiver, Jube Jr. Coming Soon: a Cellphone Directory. Los Angeles Times, May 20, 2004, p. A1 (via Factiva), citing a study by the Zelos Group Inc.

[6] See [http://www.qsent.com/news/news-2004-09-21-1.shtml].

[7] Sprint PCS, ALLTEL Cite Regulations in Deciding Not to Offer 411 Yet. TR Daily, January 14, 2005 (via Factiva).

[8] Sprint PCS, ALLTEL Cite Regulations in Deciding Not to Offer 411 Yet, Ibid.

will have to consent to having their numbers listed. Opponents counter that many subscribers do not realize that they already have given consent through the contract they sign with their service provider.[9] Other critics point out that wireless subscribers pay for every call, and view their cell phones as distinctly private. From the beginning, one of the largest mobile service providers, Verizon Wireless, decided not to participate in the directory. The company's President and CEO, Denny Strigl, argues against the notion of an "opt-in" directory, where subscribers would have to give their express prior authorization to being listed, saying that "Customers see opt-in as a disingenuous foot-in-the-door — leading to 'opt-out' clauses and fees for not publishing a number. Nor does opt-in allow customers any degree of control over how and to whom their information is revealed — they either keep full privacy or face full exposure, with nothing in-between."[10] ("Opt-in" and "Opt-out" are explained below.) Consumers Union established a website [http://www.escapecellhell.org] to encourage individuals to contact their Members of Congress in support of wireless directory legislation.

Three bills concerning wireless directories were introduced in the 108th Congress (see appendix). In September 2004, hearings were held by the Senate Commerce, Science, and Transportation Committee, and by the House Energy and Commerce Committee's Subcommittee on Telecommunications and the Internet. At the 2004 Senate hearing, CTIA testified that there is no need for legislation because the directory does not yet exist so it is premature to pass legislation now, the wireless industry has a proven track record in protecting consumer privacy, and subscribers would not be forced to participate in the directory nor charged a fee for opting-out. Mr. Strigl from Verizon Wireless repeated his strong opposition to the directory, but agreed that legislation is not necessary. Some opponents of the legislation point to Verizon's decision not to participate in the directory as indicative of a market-based solution to the problem, since subscribers wishing not to be listed could switch to Verizon.

Advocates of the legislation at the 2004 House hearing countered that, for example, the wireless industry's track record is less than perfect. According to *Communications Daily*,[11] Representative Pitts, who sponsored one of the 108th Congress bills, stated that when he first discussed a wireless directory with industry representatives two years earlier, they insisted that opt-in was impossible, and they would need to charge for the service. Yet now, he noted, the industry is asserting that the system would be opt-in and free. Representative Markey commented that the fact that the carriers informed consumers that their numbers might become listed in a wireless directory only in the fine print of their service contracts made some

---

[9] At a Senate Commerce Committee hearing on September 21, 2004, Kathleen Pierz of The Pierz Group testified that nearly all mobile subscribers, except Cingular Wireless customers, have already signed a contract that includes their express permission to have their mobile number listed in any type of directory the carrier chooses.

[10] Verizon Wireless CEO Calls for Preserving Customer Privacy and Open Competition at Yankee Group Wireless Summit. Verizon Wireless Press Release, June 21, 2004. [http://news.vzw.com/news/2004/06/pr2004-06-21.html]

[11] Carriers Promise Congress Wireless 411 Will Protect Privacy. Communications Daily, September 30, 2004, p. 2.

observers suspicious of their intentions. Senator Boxer testified at the House hearing, noting that cell phones are quite different from home phones because people take them wherever they go, so unwanted calls are even more intrusive. She emphasized the need to allow parents to control whether their children's numbers are listed, and the need to act quickly, before the directory comes into existence. Witnesses from EPIC and the AARP testified in favor of the legislation at the Senate hearing.

Other Concerns

Other wireless privacy concerns exist, but are outside the scope of this report to discuss in depth. Briefly, some are concerned about whether law enforcement authorities might require wireless carriers to provide location information.[12] CDT's James Dempsey notes that government access to data stored on a third party network is not subject to Fourth Amendment protections that require probable cause before conducting searches.[13] CDT's Alan Davidson was quoted in *Computerworld* about other ominous implications. "'The first time somebody steals location information on the whereabouts of a kid and he goes missing, there will be a backlash and lawsuits,' he added. Or a phone company employee could have a crush on a woman with a cell phone and use the purloined data to follow her around, he said."[14]

It should be noted, however, that privacy concerns in the Internet arena, at least, often are tempered by consumers' desires for new services and low prices. The extent to which consumers would choose one wireless carrier over another purely because one promised better privacy safeguards is unclear.

Fair Information Practices

Much of the wireless privacy controversy parallels the debate over Internet privacy (see CRS Report RL31408) and spam (see CRS Report RL31953). In that context, questions have arisen over whether wireless carriers should be required to follow "fair information practices" with regard to collection, use, or dissemination of call location information.

The Federal Trade Commission (FTC) has identified four "fair information practices" for operators of commercial websites: providing *notice* to users of their information practices before collecting personal information, allowing users *choice* as to whether and how personal information is used, allowing users *access* to data collected and the ability to contest its accuracy, and ensuring *security* of the information from unauthorized use. *Enforcement* is sometimes included as a fifth practice. "Choice" is often described as "opt-in" or "opt-out." To opt-in, consumers

---

[12] Some of these concerns stem from the Communications Assistance for Law Enforcement Act (CALEA). See CRS Report RL30677, *Digital Surveillance: the Communications Assistance for Law Enforcement Act*, by Patricia Moloney Figliola.

[13] Quoted in: Communications Daily, June 20, 2001, p. 3.

[14] Quoted in: Computerworld, October 2, 2000, p. 10

must give their affirmative consent to a website's information practices. To opt-out, consumers are assumed to have given consent unless they indicate otherwise.

Some argue that similar practices should be observed by wireless carriers or providers of location-based information and services. A major issue is whether Congress should pass a law requiring them to do so, or if industry self-regulation is sufficient.

Industry Efforts to Respond to Privacy Concerns

Several industry segments are involved in the wireless privacy debate: the wireless carriers required by the FCC to provide E911 capabilities; companies offering location-based information and services; and websites that can be accessed over wireless devices.

The optimism surrounding the business potential of wireless devices is exemplified by the emergence of the terms M-Commerce (mobile commerce) and L-Commerce (location commerce) and the creation of industry associations to promote them. The Wireless Location Industry Association [http://www.wliaonline.org] has developed draft wireless privacy policy standards for its members, available on the WLIA website at [http://www.wliaonline.org/indstandard/privacy.html]. The Mobile Marketing Association developed a code of conduct, which is posted on its website [http://www.mmaglobal.com/conduct/coc.html], and was adopted by MMA's Board of Directors in November 2003. Both WLIA and MMA combine opt-in and opt-out approaches. MMA has established a wireless anti-spam committee in what it calls the second phase of its efforts to ensure wireless applications are spam-free (the release of the Code of Conduct was the first phase).

TRUSTe, a company that offers privacy "seals" to websites that follow certain privacy guidelines, released what it called the "first wireless privacy standards" on February 18, 2004 [http://truste.org/pdf/TRUSTe_Wireless_Privacy_Principles.pdf]. The "Wireless Privacy and Principles and Implementation Guidelines" call for —

- wireless service providers to give notice to their customers prior to or during the collection of personally identifiable information (PII), or upon first use of a service;
- wireless service providers to disclose customers' PII to third parties only if the customer has opted-in, and the customer should be able to change that preference at any time; and
- wireless service providers may only use location information for services other than those related to placing or receiving calls if the customer has opted-in, and wireless service providers should disclose the fact that they retain location information beyond the time reasonably needed to provide the requested service.

As part of the announcement, TRUSTe noted that it had formed a "Wireless Advisory Committee" that includes MMA and WLIA, as well as AT&T Wireless, Microsoft, HP, PricewaterhouseCoopers, the Center for Democracy and Technology, and the Privacy Rights Clearinghouse. The committee's function is "to promote

privacy standards to increase consumer use of advanced wireless features and applications." The MMA's Code of Conduct includes a requirement to "align" with the TRUSTe principles.

The FTC held a workshop on wireless Web privacy issues in December 2000.[15] According to a media account, participants conceded that many companies developing wireless applications are too busy implementing their services to focus on privacy issues, and that since these companies are not certain of what future applications may emerge, "they tend to collect far more data than they need right now ... and even more collection is likely once there's ready buyer [sic] for information."[16] Some participants noted the importance of determining privacy requirements early in the development of wireless and location-based services so systems and equipment need not be retrofitted in the future.

In November 2000, CTIA asked the FCC to initiate a rulemaking, separate from its rulemaking on Customer Proprietary Network Information (CPNI, see discussion of the 911 Act, below), on implementation of the wireless location information amendments made by P.L. 106-81. CTIA argued that location privacy information is uniquely a wireless concern, and such an FCC rulemaking would attract commenters who would not be interested in the general CPNI rulemaking. CTIA asked that the FCC adopt privacy principles to assure that mobile services users would be informed of the location information collection and use practices of their service providers before the information is disclosed or used. Specifically, CTIA wanted the FCC to adopt technology neutral (i.e., for either handset- or network-based systems) rules requiring notice, choice, and "security and integrity." The latter phrase was described as meaning that location information should be protected from unauthorized use and disclosure to third parties, and third parties must adhere to the provider's location information practices. The FCC issued a Public Notice on March 16, 2001 requesting comments on CTIA's request.[17] After receiving comments and deliberating on the request, the FCC announced in July 2002 that it would not commence such a proceeding. The FCC concluded that the "statute imposes clear legal obligations and protections for consumers" and "we do not wish to artificially constrain the still-developing market for location-based services..."[18] The FCC added that it would closely monitor the issues and initiate a rulemaking proceeding "only when the need to do so has been clearly demonstrated."

---

[15] The transcript of the FTC's two-day (Dec. 11-12, 2000) workshop is available in two parts (day 1 and day 2) at [http://www.ftc.gov/bcp/workshops/wireless/001211.htm] and [http://www.ftc.gov/bcp/workshops/wireless/001212.htm].

[16] Communications Daily, December 13, 2000, p. 4. At the time, CTIA stood for Cellular Telecommunications Industry Association. The organization later changed its name to Cellular Telecommunications & Internet Association, and now is referred to as CTIA — the Wireless Association [http://www.ctia.org].

[17] Federal Communications Commission. Wireless Telecommunications Bureau Seeks Comment on Request to Commence Rulemaking to Establish Fair Location Information Practices. WT Docket No. 01-72. March 16, 2001. DA 01-696.

[18] Federal Communications Commission. Order. WT Docket No. 01-72. FCC 02-208. Adopted July 8, 2002; released July 24, 2002.

Existing Laws

The Telephone Consumer Protection Act (TCPA)

The 1991 Telephone Consumer Protection Act (TCPA, P.L. 102-243), *inter alia*, prohibits the use of autodialers or prerecorded voice messages to call cellular phones, pagers, or other services for which the person would be charged for the call, unless the person has given prior consent. In 2003, the FCC ruled that TCPA applies to any call that uses an automatic dialing system or artificial or recorded message to a wireless phone number, including both voice messages and text messages such as Short Message Service (SMS).[19]

The Wireless Communications and Public Safety Act (the "911 Act")

Since 1996, the FCC has issued a series of orders to ensure that users of wireless phones and certain other mobile devices can reach emergency services personnel by dialing the numbers 911. The FCC rules, referred to as "Enhanced 911" or E911, apply to all cellular and Personal Communications Services (PCS) licensees, and to certain Specialized Mobile Radio licensees. A fact sheet describing the FCC's actions is available at [http://www.fcc.gov/911/enhanced]. This report addresses only the privacy implications of the availability of the call location information that will enable wireless E911 to work. Other E911 issues, including implementation, are discussed in CRS Report RS21028 and CRS Report RS21222.

Because the technologies needed to implement E911 enable wireless telecommunications carriers to track, with considerable precision,[20] a user's location any time the device is activated, some worry that information on an individual's daily habits — such as eating, working, and shopping — will become a commodity for sale to advertising companies, for example.

In 1999, Congress passed the Wireless Communications and Public Safety Act (P.L. 106-81), often called "the 911 Act." In addition to making 911 the universal emergency assistance number in the United States, the 911 Act also amended section 222 of the Communications Act of 1934 (47 U.S.C. §222), which establishes privacy protections for **customer proprietary network information (CPNI)** held by telecommunications carriers. *Inter alia*, the 911 Act added "location" to the definition of CPNI.

---

[19] SMS is generally defined as a short (less than 160 alpha-numeric characters) message that contains no text or graphics.

[20] Under Phase 2 of E911 implementation, wireless carriers are required to provide "Automatic Location Identification" (ALI) information to PSAPs that will locate the caller's latitude and longitude within 50-300 meters (150-900 feet), depending on the technology used. (If handset-based technology is used, the caller's location must be identified within 50 meters for 67% of calls; within 150 meters for 95% of calls. If network-based technology is used, the location must be identified within 100 meters for 67% of the calls; within 300 meters for 95% of calls.)

Under section 222(h), as amended, CPNI is defined as:

> (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (b) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier, except that such term does not include subscriber list information.

Section 222 required the FCC to establish rules regarding how telecommunications carriers treat CPNI. The FCC adopted its Third Report and Order on CPNI on July 16, 2002,[21] setting forth a dual approach in which "opt-in" is required in some circumstances, and "opt-out" is permitted in others.[22]

In addition to adding location to the definition of CPNI, the 911 Act amended section 222(d)(4) regarding authorized uses of CPNI. As amended, the law determines those circumstances under which wireless carriers need to obtain a customer's prior consent to use wireless location information, and when prior consent is not required. A customer's prior consent is *not* required (section 222 (d)) —

- to provide call location information to a PSAP or to emergency service and law enforcement officials in order to respond to the user's call for emergency services;
- to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or
- to information or database management services providers solely for purposes of assistance in the delivery of emergency services in response to an emergency.

In a newly created section 222(f), the 911 Act states that, except in the circumstances listed above, *without express prior authorization*, customers shall not be considered to have approved the use or disclosure of or access to (1) call location information, or (2) automatic crash notification information to anyone other than for use in an automatic crash notification system.

The phrase "express prior authorization" is not further defined in the law, however, nor the measures telecommunications carriers must take to obtain it. H.R. 83 (see **Legislation in the 109th Congress**, below) would set such requirements.

---

[21] Federal Communications Commission. Third Report and Order and Third Further Notice of Proposed Rulemaking. CC Docket No. 96-115. Adopted July 16, 2002; Released July 25, 2002.

[22] Opt-in means that an individual's affirmative consent is required. Opt-out means that consent is assumed unless the individual indicates otherwise. A full discussion on the FCC's CPNI rules is outside the scope of this report. See the aforementioned FCC third report and order for further information.

The CAN-SPAM Act

In 2003, Congress passed a broad anti-spam bill, the CAN-SPAM Act (P.L. 108-187), which is addressed in more detail in CRS Report RL31953. The original version of the bill, S. 877, and the version passed by the Senate on October 22, 2003, did not address spam on wireless devices. The House, however, added such a provision (Sec. 14) in the version it passed on November 21, 2003. The Senate amended several provisions of S. 877, including the section on wireless spam, when it concurred with the House version on November 25, 2003. The House adopted the Senate version on December 8. The bill was signed into law by President Bush on December 16, 2003.

The law required the FCC, in consultation with the FTC, to promulgate rules within 270 days of enactment to protect consumers from unwanted "**mobile service commercial messages**" (**MSCMs**). That term is defined in the law as a commercial e-mail message "that is transmitted directly to a wireless device that is utilized by a subscriber of commercial mobile service" as defined in the 1934 Communications Act. (In this report, an MSCM is referred to as a wireless commercial e-mail message.)

The FCC announced a Notice of Proposed Rulemaking on March 11, 2004. According to *Communications Daily*,[23] during the comment period, several wireless carriers and the CTIA urged that they be exempted from the requirement to obtain express prior authorization before sending commercial messages to their customers if the customers are not charged for them, arguing that those are carrier-customer relationship issues and are protected by the First Amendment. CTIA reportedly agreed with the FCC's preliminary interpretation[24] that the CAN-SPAM Act applies only to messages sent to an e-mail address consisting of two parts, a unique user name or mailbox and a reference to an Internet domain (e.g. janedoe@wirelesscarrier.com), and therefore should not apply to SMS, short code or other text messages sent using other address formats.

The FCC adopted the new rules on August 4, 2004; they were released on August 12.[25] Most went into effect on October 18, 2004, although several that deal with information collection requirements must obtain approval of the Office of Management and Budget. The FCC took the following actions:

- Prohibited sending wireless commercial e-mail messages unless the individual addressee has given the sender express prior authorization ("opt-in"), which may be given orally or in writing, including

---

[23] Wireless Industry Asks for Exemption From Seeking Opt-In Consent. Communications Daily, May 4, 2004, p. 4.

[24] See paragraph 10 of the FCC's NPRM.

[25] Federal Communications Commission. FCC Takes Action to Protect Wireless Subscribers from Spam. Press Release, August 4, 2004. [http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-250522A3.pdf]. The rules were released on August 14, 2004, and are available at the website of the FCC's Office of Consumer and Governmental Affairs [http://www.fcc.gov/cgb/]. CG Docket No. 04-53 and CG Docket No. 02-278.

electronically. Requests for such authorization may not be sent to a wireless subscriber's wireless device because of the potential costs to the subscriber for receiving, accessing, reviewing and discarding such mail. Authorization provided to a particular sender does not entitle that sender to send wireless commercial e-mail messages on behalf of third parties, including affiliated entities and marketing partners. The request for authorization must contain specified information, such as the fact that the recipient may be charged by their wireless service provider for receiving the message, and subscribers may revoke their authorization at any time.

The rules do not apply to —

messages that are forwarded by a subscriber to his or her own wireless device (although they do apply to any person who receives consideration or inducement to forward the message to someone else's wireless device), or

phone-to-phone SMS messages if they are not autodialed (Internet-to-phone SMS messages *are* covered by the rules since they involve a domain name address).

- Announced that it would create a publicly available FCC wireless domain names list with the domain names used for mobile service messaging so that senders of commercial mail can determine which addresses are directed at mobile services, and —

  Prohibited sending any commercial message to addresses that have been on the list for at least 30 days, or at any time prior to 30 days if the sender otherwise knows that the message is addressed to a wireless device, and

  Required all wireless service providers to supply the FCC with the names of all Internet domains on which they offer mobile service messaging services.

- Determined that all autodialed calls, including SMS, are already covered by the TCPA.

- Interpreted the definition of wireless commercial e-mail message to include any commercial message sent to an e-mail address provided by a wireless service provider (formally called a "commercial mobile radio service," or CMRS) specifically for delivery to the subscriber's wireless device.

- Provided guidance on the definition of "commercial," but noted that the Federal Trade Commission is ultimately responsible for determining the criteria for "commercial" and "transactional or relationship" messages.

As noted, some wireless service providers sought an exemption from the requirement to obtain express prior authorization for them to communicate with their own subscribers, as long as the subscribers did not incur additional costs. The FCC did not grant such as exemption, in part because it concluded that the existing exemption in the CAN-SPAM Act for transactional or relationship messages is sufficient to cover many types of communication needed between a provider and a subscriber. Furthermore, the Commission concluded that the CAN-SPAM Act required it to protect consumers from unwanted commercial messages, not only those that involve additional costs.

Legislation in the 109th Congress

Congress continues to consider whether additional legislation is needed to protect wireless subscribers. Legislation was considered in the 108th Congress (see appendix), but none cleared Congress other than the CAN-SPAM Act, discussed above. In the 109th Congress, Representative Frelinghuysen has reintroduced a bill that he sponsored in the 108th Congress, specifying what carriers must do to obtain the "express prior authorization" required by the 911 Act. No legislation regarding wireless 411 directories has been introduced yet, but Representative Pitts indicated in a January 13, 2005 press release[26] that he plans to reintroduce a bill he offered last year (see appendix).

Wireless Privacy: H.R. 83 (Frelinghuysen)

H.R. 83 in the 109th Congress is identical to H.R. 71 from the 108th Congress. It amends the Wireless Communications and Public Safety Act to require that wireless carriers provide notice, choice, and security. It states that a customer will not be considered to have granted express prior authorization unless the carrier provides the customer, in writing, a clear, conspicuous, and complete disclosure of the carrier's practices regarding collection and use of location information, transaction information, and automatic crash identification information, before any such information is disclosed or used. The disclosure must include a description of the specific types of information collected by the carriers, how the carrier uses such information, and what information might be shared or sold to other companies and third parties. The customer must agree in writing to the collection and use of such information, or agree to its collection and use subject to certain limitations. The carriers must establish and maintain procedures to protect the confidentiality, security, and integrity of the information. The FCC is responsible for developing regulations to implement these amendments. The bill was referred to the House Energy and Commerce Committee.

---

[26] Sprint Opts Out of Wireless Directory. Press Release from the Office of Congressman Joe Pitts, January 13, 2005. [http://www.house.gov/pitts/press/releases/050113r-sprint.htm]

Appendix: Legislative Action in the 108th Congress

The 108th Congress passed, and the President signed into law, the CAN-SPAM Act (P.L. 108-187) which includes provisions related to wireless spam. Four other bills were introduced: H.R. 71 (Frelinghuysen), H.R. 3558 (Pitts), S. 1963 (Specter) and S. 1973 (DeWine). None of these cleared Congress.

Wireless Privacy: H.R. 71 (Frelinghuysen)

H.R. 71 would have amended the Wireless Communications and Public Safety Act to require that wireless carriers provide notice, choice, and security. It stated that a customer would not be considered to have granted express prior authorization unless the carrier provided the customer, in writing, a clear, conspicuous, and complete disclosure of the carrier's practices regarding collection and use of location information, transaction information, and automatic crash identification information, before any such information is disclosed or used. The disclosure would have had to include a description of the specific types of information collected by the carriers, how the carrier uses such information, and what information might be shared or sold to other companies and third parties. The customer would have had to agree in writing to the collection and use of such information, or agree to its collection and use subject to certain limitations. The carriers would have had to establish and maintain procedures to protect the confidentiality, security, and integrity of the information. The FCC would have been responsible for developing regulations to implement these amendments. The bill was referred to the House Energy and Commerce Committee. There was no further action. This bill has been reintroduced in the 109th Congress as H.R. 83.

"Wireless 411" Directory Assistance: H.R. 3558 (Pitts), S. 1963 (Specter), and S. 1973 (DeWine)

H.R. 3558, S. 1963 and S. 1973 were virtually identical bills, each entitled "Wireless 411 Privacy Act." The bills would have enabled wireless subscribers to choose to keep their wireless telephone numbers unlisted, for free, if a directory assistance database for wireless subscribers is created. CTIA, is assembling such a database (discussed above).[27] The legislation would have required commercial mobile service providers to obtain express prior authorization ("opt-in") from each current subscriber, separate from any authorization obtained to provide the subscriber with mobile service or any associated calling plan or other service, to include the subscriber's wireless phone number in the database. For new subscribers, mobile service providers would have had to provide a separate notice at the time a new subscriber signed up for service, and at least once a year thereafter, informing the subscriber of the right not to be listed, and providing a convenient mechanism for the subscriber to decline or refuse to be listed ("opt-out"). Call forwarding from a directory assistance operator to a subscriber would have been permitted only if the operator first informed the subscriber of who was calling and the subscriber could

---

[27] Shiver, Jube. Coming Soon: A Cellphone Directory. Los Angeles Times, May 20, 2004, A-1 (via Factiva).

accept or reject the incoming call on a per-call basis, and the subscriber's phone number would not have been disclosed to the calling party. Call forwarding would not have been permitted to subscribers whose numbers were unlisted. The bills would also have prohibited commercial mobile service providers from publishing, in print, electronic, or other form, the contents of any wireless directory assistance database. No fees could have been charged to subscribers for keeping their phone numbers private. H.R. 3558 was referred to the House Energy and Commerce Committee, and S. 1963 and S. 1973 to the Senate Commerce, Science, and Transportation Committee.

The Senate Commerce Committee held a hearing on S. 1963 on September 21, 2004. The bill was marked up the next day. After considerable debate, and adoption of a Boxer substitute amendment, the bill was ordered reported (12-10). A written report was filed on December 7, 2004 (S.Rept. 108-423). There was no further action in the Senate.

The House Energy and Commerce Committee held a hearing on this topic on September 29, 2004. There was no further action in the House.

The House and Senate committee hearings are discussed in the main text of this report (see **"Wireless 411" Directories**).