Order Code RL31636

CRS Report for Congress

Received through the CRS Web

Wireless Privacy and Spam: Issues for Congress

Updated September 1, 2006

Patricia Moloney Figliola
Specialist Telecommunications and Internet Policy
Resources, Science, and Industry Division

GalleryWatch.com
http://www.crsdocuments.com
Penny Hill Press

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, primarily in the areas of CPNI, wireless location data, and proposed wireless directory assistance services.

Note: This report was originally written by Marcia S. Smith; the author acknowledges her contribution to CRS coverage of this issue area.

Contents

Introduction 1

Concerns of Consumers and Privacy Rights Advocates 2
- Spam 2
- "Wireless 411" Directory 3
- Selling Cell Phone Records 5
  - EPIC Filings with the FTC and FCC 5
  - FTC and FCC Actions 6
  - Reaction from Sellers of Cell Phone Information 7
  - Reaction from the Telecommunications Industry 7
  - Congressional Response 7
- Other Concerns 9

Fair Information Practices 9

Industry Efforts to Respond to Privacy Concerns 10

Existing Laws 12
- The Telephone Consumer Protection Act (TCPA) 12
- The Wireless Communications and Public Safety Act (the "911 Act") 13
- The CAN-SPAM Act 14

Legislation in the 109th Congress 17
- Wireless Location Information Privacy 17
- Wireless Directory Assistance Services ("Wireless 411") 17
- Customer Proprietary Network Information (Customer Records) 18

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 RL32939, *An Emergency Communications Safety Net: Integrating 911 and Other Services*, 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. Further legislation is pending in the 109th Congress.

Concerns of Consumers and Privacy Rights Advocates

Spam

Some consumers and privacy rights groups, including the Center for Democracy and Technology (CDT)[5] and the Electronic Privacy Information Center (EPIC),[6] 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.

[5] The CDT website is [http://www.cdt.org].

[6] The EPIC website is [http://www.epic.org].

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" Directory

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 CTIA — The Wireless Association,[7] began developing one in 2004 for six of the seven largest mobile service providers.[8] 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.[9] Qsent is the "aggregator" for the directory service.[10]

In early 2005, some of the companies backing the directory project announced changes in their plans. Sprint and ALLTEL were the first to indicate that they would delay offering such a service until the regulatory climate stabilized. Some cited a new California law that requires carriers to obtain separate authorization from subscribers before including them in the directory as an example of the evolving regulatory climate. A number of other states are considering similar legislation. By the end of April 2005, T-Mobile reportedly was the only major carrier still planning to offer directory services, pledging to do so on an opt-in basis.[11]

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,[12] 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.)

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

---

[7] The letters CTIA once stood for Cellular Telecommunications and Internet Association, but the organization apparently now prefers to be referred to as CTIA — the Wireless Association. The CTIA website is [http://www.ctia.org].

[8] ALLTEL, Cingular Wireless, AT&T Wireless, Nextel, Sprint, and T-Mobile participated in this process (Sprint and Nextel subsequently merged). The seventh carrier, Verizon Wireless, declined to participate (discussed below).

[9] 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.

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

[11] Van, Jon. "Calls for Wireless 411 Are Fading Out," *Chicago Tribune*, April 30, 2005, p. 1 (via Factiva).

[12] The Do Not Call website is [http://www.ftc.gov/donotcall].

if they want an unlisted number). Proponents of the directory insist that customers 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.[13] 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."[14] ("Opt-in" and "Opt-out" are explained below.) Consumers Union established a website[15] to encourage individuals to contact their Members of Congress in support of wireless directory legislation.

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. (See the **Appendix** for legislation that was pending in the 108th Congress, at the time of these hearings.) 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 Wireless'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 Wireless.

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*,[16] 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

---

[13] 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.

[14] 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]

[15] See [http://www.escapecellhell.org].

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

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 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.

Legislation has been reintroduced in the 109th Congress, as discussed later in this report.

Selling Cell Phone Records

Concern is mounting about the public availability of cell phone records, which may include detailed information on calls to and from a particular number, such as the number dialed, the duration, and the location of the cell phone. Some of these records, along with records from other telephone and voice communications, may become available for sale over the Internet from "data brokers" who collect and sell the information. Attention is focused on how the data brokers obtain the information, and whether telecommunications companies are adequately protecting the so-called Customer Proprietary Network Information (CPNI) as required by law. For more discussion of CPNI, see **The Wireless Communications and Public Safety Act (the "911 Act")** below.

From a legislative standpoint, a fundamental issue is whether existing laws — the Federal Trade Commission (FTC) Act (15 U.S.C. §§ 41-51), which bans unfair and deceptive practices that might be employed by pretexters, and the 1996 Telecommunications Act, which requires telecommunications carriers to protect CPNI — are adequate, or if new laws are needed to criminalize specifically the fraudulent acquisition and sale of cell phone (or all telephone) records. Generally, privacy rights groups want additional legislation. One telecommunications association (CTIA) supports new legislation to criminalize obtaining phone records by fraudulent means. Another (USTelecom) wants improved enforcement of existing laws instead of new laws. The FCC supports three potential legislative actions: making the commercial availability of consumers' phone records illegal, overturning a 1999 court ruling that limited the FCC's ability to implement more stringent protections of consumer phone record information, and strengthening the FCC's enforcement tools. The FTC has not endorsed new laws, but recommends a multi-faceted approach that includes coordinated law enforcement by government agencies and telephone carriers, outreach to educate consumers and industry, and improved security measures by record holders.

EPIC Filings with the FTC and FCC. In July 2005, EPIC filed a complaint with the FTC regarding the sale of cell phone records by a company named Intelligent e-Commerce, Inc. (IEI), which operates the bestpeoplesearch.com

website.[17] Among the charges was that IEI was violating section 222 of the 1996 Telecommunications Act (47 U.S.C. §222) by selling information about cell phone calls made by subscribers, including billing records and other data defined as CPNI. Current law requires telecommunications carriers to protect the confidentiality of CPNI. EPIC later expanded its request to the FTC, asking for an industry-wide investigation. An IEI spokesman described the company as a customer-service and billing agency for licensed private investigators and was not aware that it was breaking any laws.[18]

EPIC's original complaint focused on the actions of IEI in obtaining the records, asserting that it only could have done so through unfair and deceptive practices, which are under the FTC's jurisdiction. Subsequently, EPIC filed a petition[19] with the Federal Communications Commission (FCC) as to whether telecommunications carriers are adequately safeguarding those records as required by law.

FTC and FCC Actions. According to the January 17, 2006 edition of *TR Daily*, in November 2005, Representative Markey asked the FCC and the FTC to act to stop the sale of cell phone subscribers' records.[20] *TR Daily* reported that in a December 13, 2005 letter to Mr. Markey, FTC Chairman Deborah Platt Majoras declined to discuss ongoing investigations, but noted that the FTC has the authority to bring a law enforcement action against a "pretexter" if it believes the pretexter's activities constitute unfair or deceptive practices as defined in the FTC Act. (Pretexters obtain consumer data by impersonating customers, employees, regulators, or others with a legitimate reason to access to the information.)

TR Daily further reported that in a January 13, 2006 letter, FCC Chairman Kevin Martin told Mr. Markey that the FCC's Enforcement Bureau is investigating the issue. On January 17, 2006, FCC commissioners Adelstein and Copps issued separate statements applauding the investigation.[21] On January 30, 2006, the Enforcement Bureau issued Notices of Apparent Liability for Forfeiture (NALs) to AT&T Wireless and Alltel for failing to certify that they have protected CPNI.[22] The Enforcement Bureau recommended $100,000 fines for each company. The FCC also issued subpoenas to several prominent data brokers seeking details on how they obtain the telephone records and asked about the sale of those records. Mr. Martin testified to the House Energy and Commerce Committee on February 1, 2006 that the data brokers did not reply adequately to the request, and that the FCC issued letters

---

[17] EPIC's complaint is available at [http://www.epic.org/privacy/iei/ftccomplaint.html].

[18] Anand, Shefali. "Privacy Group Questions Cellphone Data," *Wall Street Journal Europe*, July 11, 2005, p. A 7 (via Factiva).

[19] CC Docket No. 96-115.

[20] FCC Probing Sale of Customer Data Acquired from Phone Companies, Martin Says. TR Daily, January 17, 2006 (via Factiva).

[21] Mr. Adelstein's and Mr. Copps' statements are available on the FCC's website at, respectively, [http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-263216A1.pdf], and [http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-263222A1.pdf].

[22] The notices are available on the FCC's website [http://www.fcc.gov].

of citation to the companies and referred the inadequate responses to the Justice Department for enforcement of the subpoenas.[23] He added that the FCC subsequently issued subpoenas to an additional 30 data brokers, and, as of February 1, was awaiting their responses. He also reported that the FCC made undercover purchases of phone records from various data brokers to assist in the investigation.

Reaction from Sellers of Cell Phone Information. IEI president Noah Webster reportedly defended his company's practices by saying that cell phone records have been obtained by private investigators for a long time, and the issue is only being raised now because of privacy groups, which "often have their own agenda."[24] Mr. Webster reportedly said that subscribers could protect themselves by asking their phone company to remove call details from their bills: "I have done this personally, so I know it works. No one will be able to get your detailed phone records, because they won't exist."

According to the *Associated Press*, in January 2006, 40 websites were offering cell phone numbers, unlisted numbers, and calling records for sale.[25] The AP story reported that operators of such websites insist they are not doing anything illegal because there is no specific prohibition against pretexting to obtain another person's data unless it involves financial data (the latter would violate the Gramm-Leach-Bliley Act). Subsequently, following an FTC sweep of these sites, about 20 reportedly discontinued offering cell phone records.[26]

Reaction from the Telecommunications Industry. Four major wireless service providers (Verizon Wireless, Cingular Wireless, Sprint Nextel, and T-Mobile) have taken legal actions to stop companies that allegedly fraudulently obtain or sell their customers' cell phone records. Representatives of two major telecommunications associations — USTelecom and CTIA — testified at House and Senate hearings in 2006, as summarized below. As noted already, CTIA supports legislation to criminalize obtaining cell phone records fraudulently, while USTelecom does not support new legislation, but wants better enforcement of existing laws instead.

Congressional Response. Several bills have been introduced in the House and Senate. Each is briefly summarized at the end of the report. The House Energy and Commere Committee held a hearing on February 1, 2006, and the Senate Commerce, Science, and Transportation Subcommittee on Consumer Affairs, Product Safety, and Insurance, held a hearing on February 8, 2006. A number of

---

[23] Mr. Martin's prepared statement is available on the FCC's website at [http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-263577A1.pdf].

[24] "EPIC Asks FTC To Investigate Companies Selling Cellphone Call Records," *Communications Daily*, Janurary 17, 2006 (via Factiva).

[25] Peter Svensson. "New Demands to Halt an Old Practice: Selling Calling Records," *Associated Press*, January 18, 2006, 17:59 (via Factiva).

[26] Kerr, Jennifer C. "Web Sites Hawking Phone Records Cease Sales," *Associated Press*, February 8, 2006, 20:07 (via Factiva)

organizations were represented at both hearings: FCC, FTC, CTIA, EPIC, and PrivacyToday.com.

Witnesses from the FCC and FTC indicated that the two agencies are working collaboratively on the issue. In his prepared statement (cited previously) to the House Energy and Commerce Committee, after summarizing the actions already taken by the FCC, FCC Chairman Martin pledged to take strong action against companies that do not comply with the CPNI protection requirements. He said that EPIC's petition to open a proceeding on this matter will be acted upon formally by the FCC by February 10, 2006. Finally, he listed three actions Congress could take: make illegal the commercial availability of consumer's phone records, overturn a 1999 ruling by the 10th Circuit Court that limited the FCC's ability to implement more stringent protection of CPNI, and strengthen the FCC's enforcement tools.

FTC Commissioner Jon Leibowitz's prepared statement to the House Energy and Commerce Committee reviewed FTC's actions against pretexters, particularly in the context of enforcing the Gramm-Leach-Bliley Act that prohibits obtaining financial data through pretexting.[27] He also recounted the FTC's actions against data brokers who do not adequately safeguard data, noting that the FTC reached a settlement with data broker ChoicePoint the previous week in which ChoicePoint will pay $10 million in civil penalties and $5 million in consumer redress. That case did not involve cell phone records, however, but he explained that the FTC may bring a law enforcement action against a pretexter who obtains telephone records as an unfair and deceptive practice. Mr. Leibowitz did not make recommendations on actions Congress might take.

Other witnesses before the House committee included CTIA President Steve Largent, Robert Douglas from PrivacyToday.com, and Marc Rotenberg from EPIC. Mr. Largent and Mr. Douglas supported legislation to criminalize obtaining phone records by fraudulent means. In addition, Mr. Larson stressed that such legislation may not entirely solve the problem, while Mr. Douglas argued that the legislation should not be limited to telephone records, and that the FTC should not be given primary authority for enforcement. Mr. Rotenberg summarized his organization's efforts at raising awareness of this issue through the filings with the FCC and FTC (discussed above). He explained that telephone carriers opposed the use of enhanced security requirements for the data they collect, arguing that bringing lawsuits against pretexters would be sufficient. He insisted that enforcement alone would only drive the practice underground, and that "simple security enhancements, such as sending a wireless phone user a text message in advance of releasing records, could tip off a victim ...."[28]

Similar sentiments were offered by those witnesses or other representatives of their organizations at the Senate hearing on February 8. In addition, the House

---

[27] Mr. Leibowitz's statement is on the FTC's website at [http://www.ftc.gov/os/2006/02/commissiontestimonypretexting.pdf].

[28] Prepared statement of Marc. S. Rotenberg to the House Energy and Commerce Committee, February 1, 2006 [http://energycommerce.house.gov/108/Hearings/02012006hearing1763/Rotenberg.pdf]

committee heard from the Attorney General of Illinois, who asked that state laws not be preempted if federal legislation is enacted, and from a representative of the U.S. Telecom Association, who argued in favor of enforcement of existing laws and increased penalties, and against new security mandates. The Senate subcommittee also heard from Ms. Cindy Southworth representing the National Network to End Domestic Violence. She testified about the potential impact of the availability of stolen cell phone records and other personal information on victims of domestic violence

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.[29] 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.[30] 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."[31]

It should be noted that privacy concerns 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, *Internet Privacy: Overview and Legislation in the 109th Congress, 1st Session*, by Marcia S. Smith) and spam (see CRS Report RL31953, *"Spam": An Overview of Issues Concerning Commercial Electronic Mail*, by Marcia S. Smith). 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 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

---

[29] 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.

[30] Quoted in *Communications Daily*, June 20, 2001, p. 3.

[31] Quoted in *Computerworld*, October 2, 2000, p. 10

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 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 telecommunications carriers; 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 Mobile Marketing Association developed a code of conduct[32] that was adopted by MMA's Board of Directors in November 2003.[33] It combines opt-in and opt-out approaches. In September 2004, MMA established a wireless anti-spam committee in what it called 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.[34] 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

---

[32] The code of conduct is availbable online at [http://mmaglobal.com/modules/content/index.php?id=5&submenu=conduct].

[33] Another organization, the Wireless Location Industry Association (WLIA), was created at about the same time as the MMA, but no longer can be located on the Internet. WLIA also had a set of privacy principles that combined opt-in and opt-out approaches. The fate of WLIA is unclear.

[34] See [http://truste.org/pdf/TRUSTe_Wireless_Privacy_Principles.pdf].

- 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.

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.[35] 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."[36] 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.[37] 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

---

[35] The transcript of the FTC's two-day (December 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].

[36] *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].

[37] 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.

constrain the still-developing market for location-based services..."[38] 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."

Wireless privacy issues have expanded beyond the initial concerns about privacy principles and fair information practices. As discussed earlier, a major issue today is the sale of cell phone records, and four of the major wireless service providers have brought legal actions against companies that allegedly fraudulently obtain or sell their customers' cell phone records. CTIA applauded the introduction of legislation in the Senate in January 2006, but also said that prosecutors could act under existing law.[39] At the House Energy and Commerce Committee hearing on February 1, 2006, CTIA President Steve Largent again said his organization supports the need for legislation, but cautioned that it might not entirely solve the problem (discussed earlier). Verizon Wireless and T-Mobile are supporting Senator Schumer's bill.[40]

Existing Laws

Three existing laws directly address some aspects of the wireless privacy and spam debate: TCPA, the "911 Act," and the CAN-SPAM Act. They are summarized in this section. The privacy of cell phone records, an issue which has arisen quite recently, is not addressed by any of these three laws. Instead, the Federal Trade Commission Act (FTC Act) and the 1996 Telecommunications Act contain provisions relevant to that debate. They are discussed earlier in this report (see **Selling Cell Phone Records**), so that information is not repeated here.

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).[41]

---

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

[39] CTIA — the Wireless Association President and CEO Steve Largent Applauds Hill Efforts to Target Illegal Data Brokering. January 18, 2006. [http://www.ctia.org/news_media/press/body.cfm?record_id=1578]

[40] Wes Clark, Verizon, T-Mobile Endorse Schumer's Bipartisan Bill to Stop Sale of Cell Phone Call Logs to Protect Privacy of Million of Cell Phone Users. Press Release from the Office of Senator Charles E. Schumer, January 24, 2006 [http://schumer.senate.gov/SchumerWebsite/pressroom/press_releases/2006/PR21.Support%20Cell%20Bill.012406.html].

[41] SMS is generally defined as a short (less than 160 alpha-numeric characters) message that (continued...)

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.[42] 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 RL32939, *An Emergency Communications Safety Net: Integrating 911 and Other Services*, by Linda K. Moore.

Because the technologies needed to implement E911 enable wireless telecommunications carriers to track, with considerable precision,[43] 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.

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.

---

[41] (...continued)
contains no text or graphics.

[42] A fact sheet describing the FCC's actions in this area is available at [http://www.fcc.gov/911/enhanced].

[43] 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.)

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,[44] setting forth a dual approach in which "opt-in" is required in some circumstances, and "opt-out" is permitted in others.[45]

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.

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, *"Spam": An Overview of Issues Concerning Commercial Electronic Mail*, by Marcia S. Smith. 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

---

[44] 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.

[45] 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.

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*,[46] 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[47] 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.[48] 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 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

---

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

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

[48] 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 12, 2004 [http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-194A1.pdf], CG Docket No. 04-53 and CG Docket No. 02-278.

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.

Wireless Location Information Privacy

H.R. 83 (Frelinghuysen), the **Wireless Privacy Protection Act**, is identical to H.R. 71 from the 108th Congress. The bill would amend the Communications Act of 1934 to require informed customer prior written consent to the provision of wireless call location and crash information to a third party. The bill was referred to the House Energy and Commerce Committee.

S. 2130 (Schumer), would amend 18 U.S.C. § 2510(8) to include (1) within the definition of "contents" of any interception of wire, electronic, and oral communications to include contemporaneous, real-time, or prospective information regarding the physical location of a cellular telephone; and (2) within the definition of "tracking device," a cellular telephone for which the government seeks contemporaneous, real-time, or prospective information regarding its location.

Wireless Directory Assistance Services ("Wireless 411")

H.R. 1139 (Pitts), the **Wireless 411 Privacy Act**, is identical to H.R. 3558 from the 108th Congress. This bill would enable wireless subscribers to keep their wireless telephone numbers unlisted, for free, if a directory assistance database for wireless subscribers were to be created. The legislation requires 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 may include a subscriber's number in a 411 directory only if they provide a separate notice at the time a new subscriber signs 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 be permitted only if the operator first informs the subscriber of who is calling and the subscriber may accept or reject the incoming call on a per-call basis, and the subscriber's phone number may not be disclosed to the calling party. Call forwarding would not be permitted to subscribers whose numbers are unlisted. The bill also prohibits commercial mobile service providers from publishing, in print, electronic, or other form, the contents of any wireless directory assistance database. No fees may be charged to subscribers for keeping their phone numbers private. The bill was referred to the House Energy and Commerce Committee.

S. 1350 (Specter) has the same title as H.R. 1139, but the provisions are somewhat different. It does not differentiate between current and new subscribers, for example. In H.R. 1139, the opt-in requirement is only for current subscribers; new subscribers would be given the opportunity to opt-out. In S. 1350, opt-in consent is required from all subscribers. Also, in S. 1350, if a subscriber's number is listed in a 411 directory, and the subscriber wants it removed, the mobile service provider must do so without any cost to the subscriber. S. 1350 contains language similar to the call forwarding provisions of H.R. 1139 under the heading "wireless accessibility." Whereas H.R. 1139 prohibits commercial mobile service providers from publishing the contents of a wireless 411 directory, S. 1350 allows such publication if opt-in consent is obtained. Like H.R. 1139, S. 1350 specifies that no fees may be charged to subscribers for keeping their phone numbers private. S. 1350 also would preempt state and local laws that are inconsistent with the requirements in the bill; H.R. 1139 does not address that issue. S. 1350 was referred to the Senate Commerce, Science, and Transportation Committee.

S. 2389 (Allen), the **Protecting Consumer Phone Records Act** (also discussed below), would prohibit a provider of commercial mobile services from including the wireless telephone number of any subscriber in any wireless directory assistance database, or publishing such a directory, without first (1) providing a clear notice to the subscriber of the right not to be listed; and (2) obtaining express prior authorization from such subscriber for such listing. The bill would also require cost-free delisting for subscribers and prohibit provider from charging a fee to the subscriber for the exercise of such privacy rights.

Customer Proprietary Network Information (Customer Records)

S. 2177 (Durbin), the **Phone Records Protection Act**, prohibits the sale, fraudulent transfer or use of telephone records. The bill covers telecommunications carriers as defined in section 3 of the Communications Act of 1934, including any form of wireless telephone services such as cell phones, broadband Personal Communications Service (PCS), Specialized Mobile Radio (SMR) service, and successors to those services. The bill creates criminal penalties, including fines and up to 10 years in prison. Exceptions are provided for law enforcement agencies. The bill was referred to the Senate Judiciary Committee.

S. 2178 (Schumer), the **Consumer Telephone Records Protection Act**, would make it a criminal violation to obtain, or attempt to obtain, confidential phone records without authorization from the customer to whom those records relate by knowingly and intentionally making false or fraudulent statements or representations to an employee or customer of covered entities, providing false documentation to a covered entity knowing it was false, or accessing customer accounts via the Internet. The bill covers telecommunications carriers as defined in Section 3 of the Communications Act of 1934, and any provider of IP-enabled voice service. (IP means Internet Protocol.) The bill also prohibits any person, including employees of telephone companies or data brokers, from knowingly and intentionally selling such records without authorization from the customer. Violators would be fined, imprisoned for no more than five years, or both. Exceptions are provided for law

enforcement agencies. The bill creates enhanced penalties if the violation is committed while violating another law or as part of a pattern of illegal activity involving more than $100,000 or more than 50 customers in a 12-month period. The enhanced penalty would double the fine and allow imprisonment for up to 10 years. The bill was referred to the Senate Judiciary Committee.

S. 2264 (Pryor), the **Consumer Phone Record Security Act**, would make it unlawful for a person to: (1) obtain, or attempt to obtain, through fraud an individual's CPNI, or cause, or attempt to cause, an individual's CPNI to be disclosed to another person without authorization; (2) sell, or offer for sale, a person's CPNI without their authorization; or (3) request another person to obtain a person's CPNI from a telecommunications carrier without proper authorization (with an exception authorizing a law enforcement official to obtain a person's CPNI provided certain conditions are met). The bill would assign enforcement of the requirements of the bill to the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), and the states, and authorize a person whose CPNI has been obtained, used, or sold to file an action for civil relief against the violator. Finally, the bill would amend the Communications Act of 1934 to require telecommunications carriers to implement certain measures to protect a person's CPNI. The bill was referred to the Senate Committee on Commerce, Science, and Transportation.

S. 2389 (Allen), the **Protecting Consumer Phone Records Act**, would make it unlawful for a person to: (1) acquire or use a an individual's CPNI without written consent; (2) misrepresent that another person has consented to the acquisition of CPNI in order to obtain such information; (3) obtain unauthorized access to data processing systems or records in order to obtain such information; (4) sell, or offer to sell, CPNI; or (5) request that another person obtain CPNI from a telecommunications carrier or Internet Protocol-enabled voice service provider, knowing that the other person will obtain such information in an unlawful manner. The bill does provide for some exceptions while also providing for both civil and criminal penalties for violations. The bill would require enforcement by the FTC, the FCC, and the states, and preempt contrary state law. It would also require the FTC and FCC to conduct a public awareness campaign about protecting CPNI.

H.R. 4657 (Lipinski), the **Secure Telephone Operations Act**, would make it a crime to knowingly sell CPNI. Violators would be subject to fines or imprisonment for up to 10 years, or both. It was referred to the House Judiciary Committee.

H.R. 4662 (Blackburn), the **Consumer Telephone Records Protection Act**, has the same title as S. 2178, but is different. Section 3 would make it unlawful for any person to obtain or cause to be disclosed (or attempt to do so) CPNI by making false, fictitious or fraudulent statements or representations to an officer, employee, or agent of a telecommunications carrier; or by providing by any means, including the Internet, any document or information to an officer, employee, or agent of a telecommunications carrier knowing it was forged, counterfeit, lost, stolen, obtained fraudulently or without the customer's consent, or contained a false, fictitious or fraudulent statement or representation. It also would be unlawful to request someone to obtain CPNI knowing it would be obtained in that manner, or to sell CPNI

knowing that it was obtained by such means. Exceptions are provided for law enforcement agencies. Section 4 would require telecommunications carriers to notify customers if their CPNI was disclosed in violation of the act (that topic is not addressed in S. 2178.) The FTC would enforce Section 3. The bill sets the same criminal penalties and enhanced penalties as S. 2178. It was referred to the House Energy and Commerce Committee.

H.R. 4678 (Schakowsky), the **Stop Attempted Fraud Against Everyone's Cell and Land Line (SAFE CALL) Act**, is similar to H.R. 4662, except that it does not set criminal penalties (it would be enforced by the FTC), and does not require customers to be notified if their CPNI is disclosed. It was referred to the House Energy and Commerce Committee.

H.R. 4709 (L. Smith), the Law Enforcement and Phone Privacy Protection Act, would make it a crime knowingly and intentionally obtain, or attempt to obtain, confidential phone records information of a covered entity by making false or fraudulent statements or providing such documents, or accessing customer accounts via the Internet without prior authorization from the customer to whom the records relate. The term "confidential phone records information" is defined as information that relates to the quantity, technical configuration, type, destination, location, or amount of use of a service offered by a covered entity subscribed to by a customer of the covered entity, and is made available to a covered entity by a customer only because of the relationship between the covered entity and the customer. The term "covered entity" is defined as a telecommunications carrier (as defined in 47 U.S.C. 153) and includes any provider of IP-enabled voice service. (IP is Internet Protocol). The bill was referred to the House Judiciary Committee.

H.R. 4714 (Boswell), the Phone Records Protection Act, is identical to S. 2177. It was referred to the House Judiciary Committee. crsphpgw