WHO KNOWS WHERE YOU ARE? PRIVACY AND WIRELESS SERVICES

Ellen Traupman

Imagine a heart disease patient fitted with a monitor that calls 911 at the first sign of trouble, transports the patient's location information to the nearest public safety authority, and then forwards the patient's medical records to the appropriate emergency room.[1] Or consider the business efficiencies gained by replacing complex and costly satellite systems that track delivery fleets or traveling employees with wireless devices that use a cell phone company's location-based services.[2] Those traveling employees could be notified of nearby hotel vacancies or restaurants with available tables.[3] Back at home, parents may find comfort in equipping their teenagers with wireless phones combining location-tracking technology.[4]

Many people have criticized the advent of location-based wireless services in the United States market.[5] Location-based wireless services arrival, however, is inevitable.[6] Congress recently enacted the Wireless Communications and Public Safety Act of 1999 ("1999 Act")[7] and charged the Federal Communications Commission ("FCC") with overseeing the deployment of comprehensive end-to-end emergency communications infrastructure and programs, including "reliable wireless telecommunications networks and enhanced wireless 9-1-1 service."[8] Even prior to this congressional mandate, the FCC had established federal

[1] Shelley Emling, *You Are Here: Satellite Technology's Upcoming Products Will Allow Us to Track Kids, Pets and Stolen Cars*, DAYTON DAILY NEWS, Dec. 31, 2000, at 1L [hereinafter Emling] (describing one company's plans to market a system that uses a small chip implanted beneath a person's skin to monitor location and vital signs so that emergency help can be summoned at the first indication of trouble).

[2] Hiawatha Bray, *Something to Watch Over You*, THE BOSTON GLOBE, Jan. 22, 2001, at C1 [hereinafter Bray]; John C. Dvorak, *Somebody Will Be Watching You Eventually*, FORBES.COM, *at* http://www.forbes.com/2001/03/12/0312dvorak.html (Mar. 12, 2001) (noting the efforts of one company to create location-based systems that track and dispatch fleet vehicles, police, ambulances, school buses and taxi cabs).

[3] Simon Romero, *Location Devices' Use Rises, Prompting Privacy Concerns*, N.Y. TIMES, Mar. 4, 2001, at A1.

[4] Rick Perera, *Siemens Plans Kid-Locator Phones*, IDG.NET, *at* http://www.idg.net/crd_idgsearch_297746.html (Nov. 28, 2000) [hereinafter Perera]. Siemens has tested a wireless handset for children that allows them to access a location-monitoring call center for help. *Id.* The call center uses a "listen in" function that provides assistance to children in trouble. *Id.*

[5] *See, e.g.*, Kevin Maney, *Cellphones Could Soon Go Way Beyond Call of Duty*, USA TODAY, Aug. 23, 2000, at 3B ("You need location-based computing. I need location-based computing. We all need location-based computing. Like we need jalapeño juice rubbed into our eye sockets."); Rick Merritt, *Cellular Snoops*, ELECTRONIC ENGINEERING TIMES, *at* http://www.eetimes.com/story/editorial/OEG20001120S0018 (Nov. 20, 2000) [hereinafter Merritt] ("The cellular phone is destined to become the latest vehicle of intrusion if the government and carriers don't act quickly and responsibly.").

[6] *See* THELEN REID & PRIEST LLP, THE FCC SETS THE TABLE FOR GPS LOCATION TECHNOLOGY IN WIRELESS PHONES (authored by Daniel R. Sovocool), *at* http://www.thelenreid.com/articles/article/art_57.htm (Nov. 1999) ("A recent development in Washington has made it more likely that GPS-enabled wireless phones will evolve into the dominant telematics market over the next several years."); Andrew Kupfer, *Zeroing in on Cellular Callers*, FORTUNE, June 23, 1997, at 140 [hereinafter Kupfer] ("The cellular phone business is growing like mad, but a little-noted federal regulation will help it grow in ways that might make you think twice before hitting the SEND button."). Telematics is "[a] generic term for a wireless network supporting the collection and dissemination of data." NEWTON'S TELECOM DICTIONARY 882 (Sixteenth and a Half ed. 2000).

[7] Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286 (codified at 47 U.S.C. § 615 (Supp. V 1999)). Enacted Oct. 26, 1999, the legislation established 911 as the nationwide emergency response number for wireless telephone users and gave wireless users the benefits of enhanced 911 services previously available only to wireline callers. *See* S. REP. NO. 106-138, at 2 (1999); 47 U.S.C. § 251(e)(3) (Supp. V 1999) (The FCC "shall designate 9-1-1 as the universal emergency telephone number within the United States for reporting an emergency to appropriate authorities and requesting assistance. The designation shall apply to both wireline and wireless telephone service.").

[8] 47 U.S.C. § 615 (Supp. V 1999). Enhanced 911 service provides emergency operators with the name, address and telephone number of the caller. Because wireline callers contact Public Safety Answering Points ("PSAPs") from a fixed location, operators can dispatch emergency services to that

regulations, known as Phase II enhanced 911 ("E911"), which requires wireless carriers to upgrade their networks so that by Oct. 1, 2001, they could deliver the specific longitude and latitude of a wireless 911 caller to emergency services.[9]

The 1999 Act not only advanced the FCC's efforts to implement Phase II E911, it also amended the Communications Act of 1934 ("1934 Act")[10] to protect the confidentiality of customer proprietary network information ("CPNI")[11] derived from location-based services.[12] Following the 1999 Act, both the FCC and the Federal Trade Commission ("FTC") solicited public comment on certain privacy issues related to location-based services. In March 2001, the FCC requested comment on a set of proposed privacy principles for the wireless industry.[13] A few months earlier, the FTC hosted a workshop to discuss the impact of wireless services and emerging data technologies on location information privacy.[14]

This comment addresses fundamental privacy concerns raised by the commercial consequences of the Phase II E911 mandate.[15] First, it provides a brief explanation of how location-tracking technology works and describes ways that wireless carriers and non-carriers will use the technology to deliver location-based services. This section also provides a general overview of consumer privacy concerns that flow from using this technology. Second, this comment describes existing FCC regulations governing a telecommunications carrier's use of CPNI under Section 222 of the 1934 Act[16] and related issues pertinent to location services that government or industry have yet to address. Third, this comment discusses how non-carrier location service providers, which fall outside FCC jurisdiction, can take a proactive stance to address consumer privacy concerns by adopting reasonable self-regulatory principles. Specifically, this section focuses on privacy practices advocated by the FTC for the electronic marketplace. Finally, this comment argues that, regardless of whether additional legislation is enacted, both carriers and non-carriers should make every effort toward self-regulation in order to satisfy privacy concerns related to this new and developing technology that legislation and regulation may not have the flexibility to address.[17]

---

location. Until wireless carriers can transmit location information to PSAPs, dispatch operators have no way of knowing the location of wireless callers. *See* S. REP. NO. 106-138, at 2. Studies show that more than 43 million calls were made to 911 or other emergency services using wireless phones in 1999. CELLULAR TELECOMMUNICATIONS & INTERNET ASSOCIATION, STATISTICS & SURVEYS: WIRELESS 911 AND DISTRESS CALLS, *at* http://www.wow-com.com/industry/stats/e911 (last visited Sept. 1, 2001).

9 47 C.F.R. § 20.18(e) (2001) ("As of October 1, 2001, licensees subject to this section must provide to the designated Public Safety Answering Point the location of all 911 calls by longitude and latitude."). Citing delays in obtaining equipment and other reasons, many carriers have sought waivers of the Oct. 1, 2001, E911 implementation deadline. *See Wireless Industry Backs Requests for E911 Waivers*, TELECOMMS. REPS., Jan. 15, 2001, at 23.

10 Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (codified as amended in scattered sections of 47 U.S.C. §§ 151–710).

11 Customer proprietary network information includes "to whom, where, and when a customer places a call, as well as the types of service offerings to which the customer subscribes and the extent the service is used." Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, 64 Fed. Reg. 53,242, 53,243 (Oct. 1, 1999) (to be codified at 47 C.F.R. pt. 64); *see also* 47 U.S.C. § 222(h) (Supp. V 1999).

12 S. REP. NO. 106-138, at 8, 10. The 1999 Act added the word *location* to the definition of CPNI in 47 U.S.C. § 222(h). Section 222 of the 1934 Act protects the privacy and confidentiality of CPNI. 47 U.S.C. § 222.

13 Wireless Telecomm. Bureau Seeks Comment on Request to Commence Rulemaking to Establish Fair Location Info. Practices, *Public Notice*, 16 FCC Rcd. 5599 (2001) [hereinafter *Location Information Public Notice*]. The FCC sought comment on a petition for rulemaking submitted by the Cellular Telecommunications Industry Association, since renamed the Cellular Telecommunications & Internet Association ("CTIA") that proposed a set of privacy principles for wireless carriers offering location-based services. In their petition to the FCC, "CTIA request[ed] the adoption of privacy principles to assure wireless consumers that wireless location information will be guarded while permitting carriers to develop new and valuable location-based services. CTIA proposes the adoption of principles that provide for notice, consent and the security and integrity of wireless location information." *Id.*; *see Petition for Rulemaking* of the Cellular Telecomm. Indus. Ass'n, WT Dkt. No. 01-72 (Nov. 22, 2000) [hereinafter *CTIA Petition*].

14 FEDERAL TRADE COMMISSION, FTC WORKSHOP: THE MOBILE WIRELESS WEB, DATA SERVICES AND BEYOND: EMERGING TECHNOLOGIES AND CONSUMER ISSUES, *at* http://www.ftc.gov/bcp/workshops/wireless/index.html (Dec. 11–12, 2000) [hereinafter FTC WORKSHOP].

15 *See* Merritt, *supra* note 5.

16 47 U.S.C. § 222.

17 The U.S. Supreme Court recently stated that personal identifying information is a commodity in commerce and therefore subject to government regulation. *See* Reno v. Condon, 528 U.S. 141, 149 (2000) (holding that because an automobile driver's information is an article of commerce, the government can restrict the sale or disclosure of such information without the express authorization of the driver). Few statutes, however, directly address privacy and commercial services. Symposium, *Data Privacy Laws and the First Amendment: A Conflict?*, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 21, 22 (2000) [hereinafter Symposium]. Electronic infor-

I. HOW IT WORKS: LOCATION DETERMINATION TECHNOLOGY AND NEW WIRELESS SERVICES

In the U.S., wireless carriers must have location determination technology in place by Oct. 1, 2001, that meets specific FCC accuracy and reliability standards.[18] Some carriers have employed network-based technology that measures the direction of a wireless signal at three or more reception points to triangulate the location of a wireless signal source.[19] Carriers using network-based technology must identify a caller's location within 100 meters for 67% of all calls, and within 300 meters for 95% of all calls to be in compliance.[20] Other carriers have tested handset-based location determination technology that "requires the use of special . . . hardware and/or software in a portable or mobile phone," including Global Positioning ("GPS") devices.[21] Handset-based technology automatically relays the position of the wireless device to a location-monitoring center. Because the handset-based method is a more accurate location determination technology than triangulation, wireless carriers using handset-based solutions must identify a caller's location within fifty meters for 67% of all calls, and within 150 meters for 95% of all calls to comply with the FCC's rules.[22] In addition, some carriers are experimenting with hybrid technologies that combine both network and handset-based solutions.[23] While some location-based services only require accuracy within 100 meters, the level of accuracy required depends on the service requested.[24] Receiving a weather forecast based on location, for example, requires less accuracy than receiving navigational services.[25]

Wireless carriers face significant costs in restructuring their existing systems to meet the FCC's Phase II E911 obligations.[26] Many carriers have already spent hundreds of millions of dollars to deploy location-tracking technologies.[27] To recoup expenses, wireless carriers are exploring ways to generate new revenue from their invest-

---

mation industries that collect and use personal data are "pretty much in a self-regulatory mode" and those industries are now "trying to do the right thing." *Id.*

18 Carriers must begin selling handsets providing Automatic Location Information ("ALI") by Oct. 1, 2001. *In re* Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, *Fourth Memorandum Opinion and Order*, 15 FCC Rcd. 17,442, 17,443, para. 4 (2000) [hereinafter *E911 Fourth Memorandum Opinion and Order*]. By Dec. 31, 2001, at least 25% of all new handsets activated by a wireless carrier must be ALI-capable. By June 30, 2002, 50% of all new handsets activated must be ALI-capable, and 100% of all new digital handsets activated must be ALI-capable by Dec. 31, 2002. *Id.* at 17,444, para. 4. Carriers must reach full penetration of ALI-based handsets throughout their subscriber base by Dec. 31, 2005. *Id.*

19 Wireless Radio Services; Compatibility With Enhanced 911 Emergency Calling Systems, 64 Fed. Reg. 60,124, 60,126 (Nov. 4, 1999) (to be codified at 47 C.F.R. pt. 20). When the FCC adopted its original Phase II E911 rules in 1996, "it was believed that location information could only be effectively provided by technologies based in or overlaid on carrier networks, using approaches such as triangulation of the handset's signal." *Id.*

20 *In re* Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, *Third Report and Order*, 14 FCC Rcd. 17,388, 17,394, para. 12 (1999) [hereinafter *E911 Third Report and Order*]; 47 C.F.R. § 20.18(h)(1) (2001).

21 47 C.F.R. § 20.3 (2001).

22 *E911 Third Report and Order*, 14 FCC Rcd. at 17,392, para. 9; 47 C.F.R. § 20.18(h)(2) (2001).

23 The FCC recently granted VoiceStream Wireless an extension of the Oct. 1, 2001, deadline to deploy a hybrid-location solution involving both network and handset-based equipment "because [the FCC found] that VoiceStream's proposed system will provide meaningful public safety benefits." *E911 Fourth Memorandum Opinion and Order*, 15 FCC Rcd. at 17,442, para. 2; *see* Wireless Radio Services; Compatibility With Enhanced 911 Emergency Calling Systems, 64 Fed. Reg. at 60,127 ("While no single solution appears to be perfect in all situations, each type of solution has its advantages and limitations and each may be improved or combined with other technologies in the future to support further improvements in 911 service.").

24 LEHMAN BROTHERS, INTRODUCING THE EUROPEAN MOBILE LOCATION SERVICES MARKET 2 (2000).

25 *Id.*

26 The FCC has conditioned a carrier's obligation to transmit location information to a PSAP upon mechanisms being in place for the recovery of the PSAP's costs of implementing E911. *In re* Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, *Second Memorandum Opinion and Order*, 14 FCC Rcd. 20,850, 20,853, para. 5 (1999). This "cost recovery" rule, however, does not require cost recovery mechanisms for recapturing a carrier's costs in providing E911 service. *Id.* at 20,853, para. 4. The FCC eliminated the prerequisite that carrier cost recovery mechanisms be in place before the wireless carrier's obligation to provide E911 service is triggered because it held that such a rule would be a significant impediment to the E911 Order's schedule and service requirements. *Id.* at 20,853, para. 3. The FCC stated that it did not reject carrier self-recovery as a means to recoup costs and "by eliminating the rule for carriers, [the FCC] neither mandate[d] self-recovery as the only cost recovery option nor prohibit[ed] any other mechanism, but rel[ied] on all carriers to implement E911 within the timetable regardless of any cost recovery mechanism." *Id.* at 20,874, para. 58.

27 Ephraim Schwartz, *Privacy or Profit: Which Do You Think Will Win? Telcos Prepare for Pervasive Marketing*, INFOWORLD, Jan. 22, 2001, at 56 [hereinafter Schwartz, *Privacy or Profit*].

ments in these capabilities.[28] The same technology that alerts paramedics and police to safety emergencies, for example, can also help automobile drivers locate the nearest French restaurant or gas station.[29] Additionally merchants will be equipped to call a frequent shopper's mobile phone and offer a time-sensitive coupon when the shopper is near the merchant's store.[30] Recognizing a fast-approaching boom in the wireless location services industry, researchers estimate that the market for such services will exceed $40 billion worldwide by 2006.[31]

Carriers will likely purchase commercial location service solutions from location commerce (or "l-commerce") platform providers that integrate network-based or GPS technologies with applications and content to deliver services to an end-user wireless device.[32] Application providers develop services like news delivery, weather forecasting, restaurant or movie guides, location-based couponing and other commerce-related wireless programming. To match consumers with merchants effectively in the location services environment, application providers may develop a profile of an end-user's interests and then access content sources matching those interests with favorite products.[33] Content providers supply the news, advertising, yellow page information, traffic reports, movie reviews and other items used in delivering services to wireless devices. Ultimately, the end-user receives location-based services through a wireless PC, in-vehicle computer, mobile phone, pager, Palm device or other personal digital assistant ("PDA").

The anticipated arrival of location-based service raises concerns among federal agencies and consumer groups about protecting personal privacy in the electronic marketplace.[34] Location service providers will have incentives to collect, store and analyze information concerning customers' location and consumer usage habits.[35] For example, if a service provider knows that a particular customer repeatedly requests information about movie theatre locations, the provider could use this data to push targeted location-based coupons and ads to the frequent moviegoer.

---

28 *Id.*

29 Bray, *supra* note 2, at C1.

30 *See* Dana Hawkins, *Will Cellphones Be Stoolies?*, U.S. NEWS & WORLD REP., Nov. 27, 2000, at 74 [hereinafter Hawkins]. In a recent study by Driscoll-Wolfe Marketing & Research Consulting, only 15% of respondents expressed an interest in receiving unprompted advertising from retailers based on location, even if they could select the stores from which to receive announcements. Press Release, Driscoll-Wolfe Marketing & Research Consulting, Driscoll-Wolfe Conducts Nationwide Study on Consumer Interest in Wireless Internet Location-Based Services, *at* http://www.driscoll-wolfe.com/WILS%20PR.htm (last visited Sept. 1, 2001). Nearly 31% of respondents, however, said they would receive promotional messages in exchange for free incoming calls. *Id.* Presumably, a challenge for location service providers will be to judge the "frustration quotient" of its customers. Symposium, *supra* note 17, at 52 ("Something may be one of life's little annoyances, and we all have our list of annoyances, but depending on what one's frustration quotient is, one gets very upset, mildly upset, or not upset at all.").

31 *Location Services to Hit $40.7 Billion in 2006*, GLOBAL POSITIONING & NAVIGATION NEWS, Jan. 24, 2001 (citing an estimate reported by research firm Allied Business Intelligence).

32 L-commerce platform providers develop software and hardware systems to integrate various databases and application servers to deliver location services. Several location services platform providers have already begun marketing their systems in Europe, Asia and the United States. *See IDC Gets a Response*, ADVANCED TRANSP. TECH. NEWS, Aug. 2000 (describing the l-commerce platform of one company that obtains location information from wireless phones and interfaces with switching equipment for the proper routing of 911 calls); Press Release, ObjectFX Corporation, ObjectFX Corporation Announces Wireless Location-Commerce Services, *at* http://www.objectfx.com/news/index.asp?yr=2000&id=39 (Sept. 20, 2000) (describing ObjectFX's plans to offer access to map viewing, point-to-point routing and detailed weather information to telecommunications carriers); Press Release, LocatioNet, LocatioNet Opens Office In Manhattan, *at* http://www.locationet.com/Eng/showNewsEvents.asp?p=314 (Mar. 1, 2001) (noting l-commerce platform provider's efforts to expand into the U.S. market after serving 350,000 customers worldwide).

33 *See* Press Release, When2Click.com, Inc., When2Click.com Announces Partnership with iPal.com to Provide Time-Sensitive Content Wirelessly, *at* http://www.when2click.com/011700.html (Jan. 17, 2001). iPal, an application provider, plans to offer time-based content developed by When2Click.com, a content provider, "by using its unique matching technology to instantly deliver content to users based on highly specific profiles and exact locations." *Id.*

34 *See* FTC WORKSHOP, *supra* note 14. Privacyclue.com, a privacy consultancy group, states that coupling the FCC's E911 location-tracking technologies with "convergence of entertainment media and data services over broadband technologies (both wireline and wireless), companies in the wireless and broadband arenas will have unparalleled access to even more data about consumer behavior and interests." PRIVACYCLUE.COM, SERVICES, WIRELESS & BROADBAND, *at* http://www.privacyclue.com/services-w.html (last visited Sept. 1, 2001).

35 Alan Charles Raul, *O Customer, Where Art Thou?*, ECOMPANY NOW, Mar. 1, 2001, *available at* http://www.ecompany.com/articles/mag/0,1640,9304,00.html (last visited Sept. 1, 2001) [hereinafter Raul] ("Information like this is simply too good—not to mention expensive—to leave for emergencies and police work.").

Such practices may place consumers at the mercy of advertisers and marketers. Location service providers will likely seek ways to collect and store information and user profiles about, among other things, the customer's favorite restaurants, movies, nightclubs and retail stores.[36] Even customers that have signed up voluntarily to receive location services may remain largely oblivious as to what information is collected, how it is used, how long it is stored and with whom is it shared or sold.[37] In the wrong hands, location information could result in a stalker gaining access to a victim's position or to a missing child under location-based surveillance.[38] Combined with web browsing data and offline sources, location information may contribute to elaborate user profiling, which generates significant privacy concerns among consumers.[39] Indeed, privacy concerns over wireless services have the potential to exceed privacy concerns over the wired Internet.[40]

II. RULES FOR WIRELESS CARRIERS

A. Customer Privacy and Section 222 of the 1996 Act

1. Protecting Customer Proprietary Network Information (CPNI) before the 1996 Act

The FCC began regulating the use of and access to CPNI by telecommunications carriers in the 1980s, when CPNI became a valuable asset for marketing enhanced services[41] and customer premises equipment.[42] Because CPNI includes "virtually all information about a customer's use of network services that a [carrier] may acquire in providing those services,"[43] it holds unique competitive advantages for carriers interested in using targeted marketing practices. In the 1980s, carriers used CPNI to design communications systems and compete for customers.[44] A carrier could use aggregate CPNI on usage levels and traffic pat-

36 *See Online Profiling: Benefits and Concerns: Hearing Before the Senate Comm. on Commerce, Sci. and Transp.*, 106th Cong. (2000) (statement of Jodie Bernstein, Director of the Bureau of Consumer Protection, Federal Trade Commission) [hereinafter *FTC Statement Online Profiling*] ("Businesses clearly benefit . . . from the ability to target advertising because they avoid wasting advertising dollars marketing themselves to consumers who have no interest in their products.").

37 *See id.* (stating that the most significant concern among Internet users is that information is collected without consumers' knowledge).

38 Matt Hamblen, *Slippery Road Ahead For Wireless Location Apps*, COMPUTERWORLD, Oct. 2, 2000, at 10.

39 *See FTC Statement Online Profiling*, *supra* note 36 ("[T]he cumulation over time of vast numbers of seemingly minor details about an individual produces a portrait that is quite comprehensive and, to many, inherently intrusive.").

40 Legal scholars have suggested that the reality that personal information is accessible by others may influence individual identities in the electronic age. Symposium, *supra* note 17, at 32. Considering the power of location tracking technology to expand the amount and type of personally identifiable information available to others, location services may impact "the extent to which certain actions or expressions of identity will be encouraged or discouraged." *Id.*

41 FCC rules define "enhanced service(s)" as "services, offered over common carrier transmission facilities used in interstate communications, which employ computer processing applications that act on the format, content, code, protocol or similar aspects of the subscriber's transmittal information; provide the subscriber additional, different, or restructured information; or involve subscriber interaction with stored information." 47 C.F.R. § 64.702(a) (2000); *see In re* Amendment of Section 64.702 of the Commission's Rules and Regulations (Second Computer Inquiry), *Final Decision*, 77 F.C.C.2d 384 (Computer II Final Decision), *modified on recon.*, 84 F.C.C.2d 50 (1980) (Computer II Reconsideration Order), *modified on further reconsideration*, 88 F.C.C.2d 512 (1981), *aff'd sub nom.* Computer and Communications Indus. Ass'n v. FCC, 693 F.2d 198 (D.C. Cir. 1982), *cert. denied*, 461 U.S. 938 (1983), *aff'd on second further reconsideration*, FCC 84-190 (rel. May 4, 1984); *In re* North American Telecomm. Ass'n Petition for Declaratory Ruling Under Section 64.702 of the Commission's Rules Regarding the Integration of Centrex, Enhanced Services, and Customer Premises Equipment, *Memorandum Opinion and Order*, 101 F.C.C.2d 349 (1985), *reconsideration*, 3 FCC Rcd. 4385 (1988). Enhanced services "generally include such services as voice mail, electronic mail, electronic store-and-forward, fax store-and-forward, data processing, and gateways to online databases." PETER H. HUBER ET AL., FEDERAL TELECOMMUNICATIONS LAW 1257 n.235 (1999) [hereinafter HUBER].

42 The 1934 Act defines "customer premises equipment" ("CPE") as "equipment employed on the premises of a person (other than a carrier) to originate, route, or terminate telecommunications." 47 U.S.C. § 153(14) (Supp. V 1999). CPE includes regular residential telephone handsets, answering machines, fax machines, computer modems and other equipment that consumers and businesses use in conjunction with the network. HENK BRANDS & EVAN T. LEO, THE LAW AND REGULATION OF TELECOMMUNICATIONS CARRIERS 696–97 (1999) [hereinafter BRANDS & LEO].

43 HUBER, *supra* note 41, at 438.

44 *In re* Amendment of Sections 64.702 of the Commissions' Rules and Regulations (Third Computer Inquiry); and Policy and Rules Concerning Rates for Competitive Common Carrier Serv. and Facilities Authorizations Thereof; Communications Protocols under Section 64.702 of the Commission's Rules and Regulations, *Report and Order*, 104 F.C.C.2d 958, 1089, para. 260 (1986).

terns in specific areas to plan the technical and economic design of enhanced services.[45] Today, a carrier that collects information on customers' behaviors has an interest in using this information "to target consumers it believes might be interested in purchasing more of its services."[46]

Customer privacy was not a paramount concern when carriers entered new markets aggressively throughout the 1980s and early 1990s. At that time, the FCC and the courts clearly regarded "competitive equity" and "efficiency" as more important than privacy concerns.[47] Nevertheless, a desire for protecting customer information privacy did exist. In 1988, Judge Harold Greene[48] viewed the unique ability of the Bell Operating Companies ("BOCs") to use CPNI in developing user profiles describing customers' favorite services, times of use, monthly expenditures and usage habits as raising "very sensitive privacy questions."[49] He noted that privacy considerations were

> at stake when, for example, a [BOC], having control of its customers' lines of communication, will also have access to their lines of credit, travel plans, credit card expenditures, medical information, and the like. On the basis of a subscriber's telephone calling patterns with respect to information, a [BOC] could easily pinpoint that subscriber for the sale of [BOC]-generated information and the sale of other products and services connected therewith, to the point where that company would have a "Big Brother" type relationship with all those residing in its region.[50]

Although historically taking a back seat to competitive equity and efficiency, customer information privacy became a more important regulatory concern of the FCC in the mid-1990s. In March 1994, changes in the communications marketplace prompted the FCC to issue a public notice seeking comment on customers' CPNI-related privacy expectations.[51] At that time, local telephone companies were entering into alliances, acquisitions and mergers with non-carrier partners.[52] The FCC stated "[i]n this changing environment, access to CPNI among affiliated companies [raised] additional privacy concerns."[53]

2. *Section 222: A Legal Obligation to Protect Customer Confidentiality*

Changes in the communications service envi-

---

45 *Id.* at 1087, para. 256.

46 Brief of Amici Curiae Electronic Privacy Information Center et al. at 5, U.S. West v. FCC, 182 F.3d 1224 (10th Cir. 1999) (No. 98-9518) [hereinafter EPIC Brief].

47 *See In re* Computer III Remand Proceedings: Bell Operating Co. Safeguards and Tier 1 Local Exchange Co. Safeguards, *Report and Order*, 6 FCC Rcd. 7571, 7611, para. 86 n.159 ("[A]lthough customer privacy has always been one of the Commission's concerns in addressing CPNI, our focus in this order is on competitive equity and efficiency."); California v. FCC, 39 F.3d 919, 931 (9th Cir. 1994) [hereinafter *California I*] (holding that a FCC decision that declined to require Bell Operating Companies from obtaining prior authorization from small and residential customers was not arbitrary and capricious); SBC Communications v. FCC, 56 F.3d 1484, 1495 (D.C. Cir. 1995) (finding AT&T's use of CPNI collected by a cellular company newly merged with AT&T to market services directly to the customers of other cellular carriers was in the public interest).

48 Newly appointed to the Court of Appeals for the District of Columbia Circuit, Judge Greene inherited the federal government's 1974 antitrust case against the Bell System on his first day assigned to the bench following the 1978 death of Judge Joseph C. Waddy. HUBER, *supra* note 41, at 44, 360. Judge Greene's on-going management of the case resulted in the divestiture of Bell System into AT&T and the seven Regional Bell Operating Companies. *See* United States v. AT&T, 552 F. Supp. 131 (D.D.C. 1982) [hereinafter AT&T Consent Decree].

49 United States v. W. Elec. Co., 714 F. Supp. 1, 12 n.40 (D.D.C. 1988). In the mid-1980s, the AT&T Consent Decree prohibited the regional BOCs from providing information services to its local telephone customers. The 1934 Act defines "information service" as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications." 47 U.S.C. § 153(20) (Supp. V 1999). The District Court for the District of Columbia lifted restrictions on BOC abilities to engage in the transmission of information services, but denied requests to generate and provide content-based information services. *W. Elec. Co.*, 714 F. Supp. at 2–3. According to Judge Greene, the maintenance of user profiles and their sale or release to others were outside the scope of services included in the transmission function. *Id.* at 12 n.40.

50 United States v. W. Elec. Co., 673 F. Supp. 525, 567 n.190 (D.D.C. 1987) (citation omitted).

51 Additional Comment Sought on Rules Governing Tel. Companies' Use of Customer Proprietary Network Info., *Public Notice*, 9 FCC Rcd. 1685 (1994) [hereinafter *CPNI Public Notice*].

52 Several mergers and alliances involving telecommunications companies and other businesses commenced in the mid-1990s, including Bell Atlantic's merger with Tele-Communications Inc. (TCI), AT&T's purchase of McCaw Cellular, and U.S. West's acquisition of a significant stake in Time Warner Cable. *See generally* Kevin Maney, MEGAMEDIA SHAKEOUT 6 (1995).

> Through 1994, the revolution spread to more industries. Newspaper companies started thinking about how they might become information highway software creators. Catalog retailers ventured into electronic shopping. Wireless phone companies started realizing they could reach a mass market and push their once-expensive wireless phone service into average consumers' homes, maybe replacing traditional telephones.

Id. at 6.

53 *CPNI Public Notice*, 9 FCC Rcd. at 1685.

ronment first recognized by the FCC in 1994 became inevitable when Congress enacted the Telecommunications Act of 1996 ("1996 Act").[54] In respect to CPNI, Congress struck a new balance between privacy and competition that permitted a lower level of information sharing than had been permitted by the FCC's pre-1996 Act proceedings.[55] Congress raised the importance of consumer privacy protection in light of new competitive market forces and technologies encouraged by the 1996 Act. In turn, carriers had "a duty to protect the confidentiality of proprietary information" relating to customers under the 1996 Act.[56]

As part of the 1996 Act, Congress adopted a new Section 222 that restricted the use of CPNI obtained by telecommunications carriers in providing telecommunications services to customers.[57] Section 222 requires:

> Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.[58]

Although the requirements of Section 222 were effective immediately upon enactment of the 1996 Act in February 1996, carriers later expressed uncertainties about their CPNI responsibilities and asked the FCC to conduct a rulemaking in order to clarify their new obligations.[59] The FCC issued an order in February 1998 that implemented Section 222 as a uniform national CPNI policy ("CPNI Order").[60] The FCC concluded that carriers could use CPNI, without customer approval, "to market offerings that are related to, but limited by, the customer's existing service relationship with their carrier."[61] For all other circumstances, the FCC adopted an opt-in approach, which requires carriers to obtain express written, oral or electronic customer approval before using CPNI to market services outside the customer's existing service relationship.[62] The FCC expressly rejected an opt-out approach, "which would have required telephone customers to contact their carrier to prevent the disclosure of their personal calling records."[63]

---

54 Telecommunications Act of 1996, Pub. L. 104-104, 110 Stat. 56 (codified in scattered sections of 47 U.S.C. §§ 151–710). Congress intended the 1996 Act "to provide for a pro-competitive, de-regulatory national policy framework designed to accelerate rapidly private sector deployment of advanced telecommunications and information technologies and services to all Americans by opening all telecommunications markets to competition." S. CONF. REP. NO. 104-230, at 1 (1996). However, "[d]espite the Act's intent to be deregulatory, it has been responsible for an astonishing number of new rules and thousands of pages of FCC orders regulating the conduct of telecommunications carriers in great detail." BRANDS & LEO, *supra* note 42, at 369.

55 H.R. REP. NO. 104-458, at 205 (1996) (noting that Congress expressly intended "to balance both competitive and consumer privacy interests with respect to CPNI" in codifying the FCC's CPNI regulations in the 1996 Act); *see In re* Implementation of the Telecomm. Act of 1996: Telecomm. Carriers' Use of Customer Proprietary Network Info. and Other Customer Info., *Second Report and Order and Further Notice of Proposed Rulemaking*, 13 FCC Rcd. 8061, 8121–22, para. 77 (1998) [hereinafter *CPNI Order*].

56 47 U.S.C. § 222(a).

57 47 U.S.C. § 222. The 1996 Act defines CPNI 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.

47 U.S.C. § 222(h)(1). Congress added the word *location* in the Wireless Communications Safety Act of 1999, *supra* note 7.

58 47 U.S.C. § 222(c)(1).

59 *In re* Implementation of the Telecomm. Act of 1996: Telecomm. Carriers' Use of Customer Proprietary Network Info. and Other Customer Info., *Notice of Proposed Rulemaking*, 11 FCC Rcd. 12,513 (1996).

60 *CPNI Order*, 13 FCC Rcd. 8061. The FCC expressly preempted state laws imposing requirements inconsistent with the FCC's implementation of Section 222. *Id.* at 8078, para. 20.

61 *Id.* at 8066, para 4.

62 *Id.* at 8066–67, para. 4. "Opt-in" consent "refers to a system in which one's prior, express approval must be obtained before personal information is used for purposes beyond those associated with the initial collection purpose." Paul M. Schwartz, *Charting a Privacy Research Agenda: Responses, Agreements, and Reflections*, 32 CONN. L. REV. 929, 934 (2000) [hereinafter Schwartz, *Charting a Privacy Research Agenda*].

63 EPIC Brief, *supra* note 46, at 1. In contrast to opt-in, "opt-out . . . allows approval to be inferred from the customer-data processor relationship unless an individual specifically requests limits on further use." Schwartz, *Charting a Privacy Research Agenda*, *supra* note 62, at 934.

3. *The Tenth Circuit's Decision in* U.S. West v. FCC

Shortly after the FCC issued its CPNI Order, the Court of Appeals for the Tenth Circuit held that the FCC's implementation of Section 222 violated the First Amendment to the United States Constitution and vacated the CPNI Order.[64] The court's decision in *U.S. West v. FCC* introduced a new competitor to consumer privacy interests: the commercial speech rights of businesses seeking to communicate with their customers.[65] The Supreme Court has held that the First Amendment protects commercial speech, including advertising and marketing targeted at specific customers.[66] Following the FCC's CPNI Order, carriers argued that CPNI was speech and the FCC's restrictions implicated the First Amendment.[67]

The FCC determined that Congress left the word "approval" ambiguous in enacting Section 222 and resolved the ambiguity in its CPNI Order "by implementing the statute in a manner that [would] best further consumer privacy interests and competition."[68] Petitioner U.S. West challenged the opt-in approval process chosen by the FCC by claiming it restricted its ability to engage in commercial speech with customers.[69] The court analyzed the CPNI restrictions under a four-part test set forth in *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York* ("*Central Hudson* test").[70] First, the court determined that U.S. West's commercial speech based on CPNI was a lawful activity and was not misleading.

---

64 U.S. West, Inc. v. FCC, 182 F.3d 1224, 1228 (10th Cir. 1999), *cert. denied*, 520 U.S. 1213 (2000) ("We vacate the FCC's CPNI Order, concluding that the FCC failed to adequately consider the constitutional ramifications of the regulations interpreting § 222 and that the regulations violate the First Amendment.").

65 This comment does not address the tension between privacy and the First Amendment right of free speech, which includes protection of commercial speech. Legal scholars have noted the challenge in reconciling a consumer's right to be left alone and a business's right to communicate a marketing message. *See* Solveig Singleton, *Privacy Versus the First Amendment: A Skeptical Approach*, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 97, 97 (2000) ("The courts should think twice before sacrificing the mature law of free speech to the less coherent concerns about privacy."); Symposium, *supra* note 17, at 34 ("The challenge for justices and judges, for policy makers and legal scholars, is to construct an information privacy law that becomes an integral part of the mission of the First Amendment and not its enemy."); Andrew S. Krulwich & Bruce L. McDonald, *Evolving Constitutional Privacy Doctrines Affecting Healthcare Enterprises*, 55 FOOD DRUG L.J. 491, 509 (2000) ("The First Amendment can provide shelter for privacy claims, but it also can be their enemy.").

66 *See* Bigelow v. Virginia, 421 U.S. 809, 826 (1975) (holding that the "relationship of speech to the marketplace of products or of services does not make it valueless in the marketplace of ideas"); Va. State Bd. of Pharmacy v. Va. Citizens Consumer Counsel, 425 U.S. 748, 756 (1976) (holding that free speech protection is afforded to both the source of an advertisement and recipients of the communication); Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 570–71 (1980) (holding that a total ban on promotional advertising for a utility company violates the First Amendment because it is more restrictive than necessary to serve the state interest of conserving energy). Although the text of the First Amendment refers to laws made by Congress, it encompasses regulations promulgated by federal agencies, including the FCC. *See, e.g.*, Rust v. Sullivan, 500 U.S. 173, 177–78 (1990) (reviewing regulations promulgated by the Department of Health and Human Services under the First Amendment). Generally, courts and regulatory agencies must give deference to the intent of Congress if Congress has unambiguously addressed the precise question at issue. Chevron U.S.A. Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 842–43 (1984). If Congress has not addressed the precise question at issue or is ambiguous with respect to the issue, then the court may determine if the agency's answer is reasonable. *Id.* at 843. Deference to an agency's interpretation of a statute is generally appropriate under *Chevron*. *Id.* at 844. The Tenth Circuit, however, noted that an agency's interpretation of a statute need not be the most reasonable interpretation. *U.S. West*, 182 F.3d at 1231 (citing *Chevron*, 467 U.S. at 843 n.11). Furthermore, "deference to an agency interpretation is inappropriate not only when it is conclusively unconstitutional, but also when it raises serious constitutional questions." *Id.*

67 Dana Grantham Lennox, *Hello, Is Anybody Home? Deregulation, Discombobulation, and the Decision in U.S. West v. FCC*, 34 GA. L. REV. 1645, 1655 (2000).

68 *CPNI Order*, 13 FCC Rcd. at 8128, para. 87.

69 *U.S. West*, 182 F.3d at 1230. U.S. West also challenged the CPNI Order as effecting a "taking" under the Fifth Amendment by arguing that CPNI represented property that belonged to the carriers and the CPNI regulations greatly diminished its value. *Id.* Because the court found the CPNI regulations unconstitutional on First Amendment grounds, it did not address U.S. West's Fifth Amendment claims. *Id.* at 1239 n.14.

70 447 U.S. 557 (1980). The test articulated by the Supreme Court is as follows:

> For commercial speech to come within [protection of the First Amendment], it at least must concern lawful activity and not be misleading. Next, we ask whether the asserted governmental interest is substantial. If both inquiries yield positive answers, we must determine whether the regulation directly advances the governmental interest asserted, and whether it is not more extensive than is necessary to serve that interest.

Id. at 566.

The test is premised on a finding by the court that the activity qualifies as commercial speech. *U.S. West*, 182 F.3d at 1232. The *U.S. West* court first determined that U.S. West's usage of CPNI to target prospective customers of new or different services fit within the definition of commercial speech. *Id.* at 1232–33 (citing *Va. Bd. of Pharmacy*, 425 U.S. at 762).

ing.[71] Second, the court "assume[d] for the sake of this appeal" that the FCC asserted "a substantial interest in protecting people from the disclosure of sensitive and potentially embarrassing personal information."[72] The CPNI rules failed the third and fourth prongs of the *Central Hudson* test as applied by the *U.S. West* court. Finding that the FCC had failed to show that harm to either privacy or competition was "real," the court concluded that the opt-in regulation did not directly and materially advance the government's interest.[73] Finally, the court determined that the FCC's opt-in approval mechanism was more restrictive than necessary to serve the interest of protecting consumer privacy.[74]

Two aspects of the *U.S. West* decision merit additional discussion when considering location service privacy issues. First, the court suggested that living in a modern society requires people to accept the proposition that their personal information "is circulating the world."[75] As applied to location-based services, it is clear that there will be no market for this new industry unless end-users are willing to share some information about themselves with carriers.[76] Second, the court stated that an opt-out approval mechanism is a less restrictive alternative than the opt-in method for CPNI regulations to serve the government's interest in protecting customer privacy.[77] The court found that the FCC failed to adequately consider an opt-out alternative, and instead had "merely speculate[d] that there are a substantial number of individuals who feel strongly about their privacy, yet would not bother to opt-out if given notice and the opportunity to do so."[78] The court rejected the FCC's self-asserted reliance on "common sense judgment based on experience" in promulgating the CPNI regulations because the effectiveness opt-in or opt-out approval mechanisms could have been measured or otherwise quantitatively defined.[79]

Perhaps the Tenth Circuit's opinion merely represented an example of holding the FCC "to standards of reasoned decisionmaking and constitutional norms."[80] To privacy advocates, however, the decision "could effectively prevent the adoption of legislative safeguards that would preserve the reasonable expectation of privacy in private communications and personal activities" at a time when telephone companies, Internet service providers and other firms acquire more detailed information from customers in the course of providing service.[81] Both the Tenth Circuit and the Supreme Court denied further review of the case.

---

71 *U.S. West*, 182 F.3d at 1234.

72 *Id.* at 1236. The court had reservations as to whether the government adequately satisfied the second prong of the *Central Hudson* test "by merely asserting a broad interest in privacy." *Id.* at 1234–35. The court did not find that the FCC asserted a substantial state interest in promoting competition, stating "[w]hile we believe that the asserted interest in increasing competition would not suffice, by itself, to justify the FCC's rule, we will, in this case, consider it in concert with the government's interest in protecting consumer privacy." *Id.* at 1237.

73 *Id.* at 1237.

74 *Id.* at 1238.

75 The court distinguished the privacy interest at issue in the case from the constitutional right to privacy, as articulated in such cases as *Griswold v. Connecticut*, 381 U.S. 479 (1965) and *Roe v. Wade*, 410 U.S. 113 (1973) as a personal right deemed "fundamental" or "implicit in the concept of ordered liberty." *U.S. West*, 182 F.3d at 1234 n.6 (citing *Griswold*, 381 U.S. at 484–86 and *Roe v. Wade*, 410 U.S. at 152–56). The court stated:

> In the context of a speech restriction imposed to protect privacy by keeping certain information confidential, the government must show that the dissemination of the information desired to be kept private would inflict specific and significant harm on individuals, such as undue embarrassment or ridicule, intimidation or harassment, or misappropriation of sensitive personal information for the purposes of assuming another's identity. Although we may feel uncomfortable knowing that our personal information is circulating the world, we live in an open society where information may usually pass freely.

Id. at 1235.

76 According to the Tenth Circuit, information privacy is not a substantial state interest merely because of a general level of discomfort consumers may experience from knowing that people can access their personal information. *Id.* at 1235.

77 *Id.* at 1238–39.

78 *Id.* ("Even assuming that telecommunications customers value the privacy of CPNI, the FCC record does not adequately show that an opt-out strategy would not sufficiently protect customer privacy."). In *FCC v. National Citizens Commission for Broadcasting*, 436 U.S. 775 (1978), the Supreme Court allowed the FCC to use its common sense judgment based on experience, notwithstanding the rulemaking record, to promulgate regulations because the agency's conclusions regarding "elusive concepts, [were] not easily defined let alone measured without making qualitative judgments." *U.S. West*, 182 F.3d at 1239 (quoting *Nat'l Citizens*, 436 U.S. at 796–97).

79 *U.S. West*, 182 F.3d at 1239.

80 Bryan N. Tramont, *Too Much Power, Too Little Restraint: How the FCC Expands Its Reach Through Unenforceable and Unwieldy "Voluntary" Agreements*, 53 FED. COMM. L.J. 49, 51 (2000).

81 EPIC Brief, *supra* note 46, at 10–11. The Electronic Privacy Information Center suggested that opt-out is ineffective because the majority of the general public is unaware of

B. Section 222 and Location Services

1. Section 222 Remains the Law of the Land

Because the Tenth Circuit only nullified the FCC's interpretation of Section 222, and not Section 222 itself, the provision continues to restrict carriers' use of location CPNI.[82] In October 1999, Congress amended Section 222 to address privacy issues generated by the Wireless Communications and Public Safety Act. This new law added the word *location* to the definition of "customer proprietary network information" so that information relating to a customer's location is now protected under Section 222.[83]

Location information privacy has already received special treatment from Congress. The Wireless Communications and Public Safety Act directly addressed a carrier's authority to use wireless location information in a new Section 222(f):

> For purposes of subsection (c)(1), without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to — (1) call location information concerning the user of a commercial mobile service . . . or (2) automatic crash notification information to any person other than for use in the operation of an automatic crash notification system.

Under new Section 222(f), wireless callers must give "express prior authorization" before a carrier can use or disclose location information in non-emergency circumstances. Unfortunately, Section 222(f) provides no definition for "express prior authorization," nor does it indicate whether prior authorization involves an opt-in or opt-out standard.

2. Interpreting Amended Section 222: Implied Consent and Emergency Services

Section 222 distinguishes between emergency services and commercial services for the purpose of obtaining wireless customer consent to disclose location information. For E911 services, wireless subscribers are presumed to have given implied consent to the release of their location information to a PSAP.[84] The concept of implied consent raises its own privacy concerns in some E911 contexts. For example, a person calling 911 to report a crime or accident in which she is not involved is presumed, under Section 222, to have consented to releasing her location information, even though she does not need assistance from public safety personnel. In this context, the lack of location privacy may be a deterrent to otherwise socially valuable actions, like reporting crimes.

The Department of Justice ("DOJ") also has suggested that wireless callers give implied consent to location information disclosure to public safety authorities "because a caller who dials 911 has neither an actual nor a reasonable expectation of privacy with regard to his whereabouts at the time of the call."[85] The Communications Assistance for Law Enforcement Act of 1994 ("CALEA") requires carriers to ensure that their equipment is capable of permitting the government, pursuant to a court order or other lawful authorization, to access certain "call-identifying information" that is reasonably available to the carrier.[86] The DOJ concluded that CALEA did not prohibit wireless carriers from transmitting information regarding the physical location of cellular telephone callers to public safety agencies.[87] Similarly, part of the Electronic Communications Privacy Act of 1986 ("ECPA") requires wireless carriers to obtain a warrant or court order before disclosing to governmental authorities information relating to wireless customers.[88] The DOJ concluded that this ECPA provision also permit-

---

the uses of their personal information and the availability of opt-out choices. *Id.* at 14–15 (citing PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION 329–30 (1996)).

82 *See* 47 U.S.C. § 222(h)(1)(A). Both the Wireless Bureau and the Common Carrier Bureau at the FCC are likely to examine how location information privacy should be protected in future CPNI rulemakings. *CTIA Seeks Uniform Policy on Location Information, Privacy,* MOBILE COMM. REP., Oct. 30, 2000; *see also Location Information Public Notice,* 16 FCC Rcd. at 5599.

83 S. REP. NO. 106-138, at 8, 10 (1999).

84 Section 222(f) suggests that approval for disclosure to public safety officials involved in an automatic crash notification system is implied by prohibiting location information use and disclosure "to any person other than" public safety personnel. 47 U.S.C. § 222(f)(2).

85 UNITED STATES DEPARTMENT OF JUSTICE, TRANSMISSION BY A WIRELESS CARRIER OF INFORMATION REGARDING A CELLULAR PHONE USER'S PHYSICAL LOCATION TO PUBLIC SAFETY ORGANIZATIONS, MEMORANDUM OPINION FOR THE ACTING ASSISTANT ATTORNEY GENERAL CRIMINAL DIVISION, *at* http://www.usdoj.gov/olc/crimfcc.htm (Sept. 10, 1996) [hereinafter DOJ MEMORANDUM].

86 47 U.S.C. § 1002(a)(2) (1994). "Call-identifying information" means "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." *Id.* at § 1001(2).

87 DOJ MEMORANDUM, *supra* note 86.

88 18 U.S.C. § 2703(a) (1994).

ted wireless carriers to transmit the location information of callers dialing 911 to public safety officials.[89]

Because 911 callers have traditionally not enjoyed a "reasonable expectation of privacy,"[90] the implied consent provision of Section 222 for disclosing location information to PSAPs may not generate too much controversy. In Europe, the Directorate-General Information Society of the European Commission has also tended to override its "prior consent" principle for disclosing of location data where emergency services use that information.[91] Requiring prior consent from a 911 caller, before using the caller's location information to dispatch emergency services, would contradict the objective of enhanced 911 services, even if some 911 callers merely report criminal activity and do not themselves need assistance.

3. *The Meaning and Implementation of "Express Prior Authorization" in Section 222*

For commercial wireless location services, resolving the consent issue will likely turn on the interpretation and implementation of "express prior authorization" in Section 222(f). The concept of "choice" has become a major principle of modern privacy law, which reflects the idea that consumers should choose what happens to their personally identifiable information.[92] Generally, consumers decide whether personal information is collected from them after receiving notice of how their information will be used by the data collector.[93] "Express prior authorization" reflects "choice" in that a customer chooses whether to allow carriers to disclose their CPNI to third parties for purposes other than the provision of services.

Although the debate historically focused largely on whether "choice" is accomplished better by opt-in or opt-out mechanisms,[94] Congress has eliminated this debate in the location services context by requiring more than mere "approval" for the use and disclosure of location-derived CPNI.[95] In *U.S. West*, the case turned on whether the FCC had determined correctly that Congress required the opt-in form to implement Section 222's "approval" requirement for using CPNI.[96] The FCC considered and dismissed an opt-out mechanism as a possible meaning of the word *approval*,[97] although the Tenth Circuit majority determined that an opt-out approach would have imposed substantially fewer restrictions on carriers' commercial speech rights.[98] An opt-out mechanism results in considerably more implied customer approvals for CPNI usage, which is increasing the carrier's marketing success.[99] Im-

89 DOJ MEMORANDUM, *supra* note 86.

90 An individual has a "reasonable expectation of privacy" when she "exhibits an actual, subjective expectation of privacy and society is prepared to recognize that expectation as reasonable." Brief of Amici Curiae National Association of Criminal Defense Lawyers and the American Civil Liberties Union at 3, Kyllo v. United States, 531 U.S. 955 (2000) (No. 99-8508); *see* Katz v. United States, 389 U.S. 347 (1967) (Harlan, J., concurring) (stating that an enclosed telephone booth, like a home but unlike an open field, is an area where "a person has a constitutionally protected reasonable expectation of privacy").

91 EUROPEAN COMMISSION DIRECTORATE-GENERAL INFORMATION SOCIETY, WORKING DOCUMENT: THE PROCESSING OF PERSONAL DATA AND THE PROTECTION OF PRIVACY IN THE ELECTRONIC COMMUNICATIONS SECTOR 4, *at* http://europa.eu.int/ISPO/infosoc/telecompolicy/review99/wdprot.pdf (Apr. 27, 2000).

92 Symposium, *supra* note 17, at 22; *see* FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS 4 (May 2000) *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf [hereinafter FTC REPORT TO CONGRESS].

93 FTC REPORT TO CONGRESS, at 4. "Notice" is the first of four widely accepted fair information practices established by the FTC, and it stands for the proposition that data collectors should notify consumers as to the information they collect, how it is collected, how it is used and whether it is disclosed to third parties. *Id.* at iii.

94 Symposium, *supra* note 17, at 22. An opt-in regime demands that the carrier not collect and use CPNI for purposes other than providing service, unless it obtains the customer's consent beforehand. Under an opt-out approach, the carrier may collect and use CPNI for marketing and other purposes, unless the customer specifically states otherwise. *See U.S. West*, 182 F.3d at 1230.

95 47 U.S.C. § 222(f).

96 *U.S. West*, 182 F.3d at 1230. Section 222 requires a carrier to obtain "the approval of the customer" before using CPNI for any purpose outside the customer-carrier service relationship. 47 U.S.C. § 222(c)(1).

97 *CPNI Order*, 13 FCC Rcd. at 8131, para. 92 ("[W]e are not persuaded that use of the term 'affirmative' in section 222(c)(2) suggests that the absence of such a term in section 222(c)(1) evinces Congressional support for an opt-out method because a common sense interpretation of 'approval' suggests a knowing acceptance, which opt-out cannot ensure."); *see* EPIC Brief, *supra* note 46, at 14 ("It is clear from reading the CPNI Order that the FCC did not casually or arbitrarily select the opt-in over the opt-out approach as though it were flipping a coin.").

98 *U.S. West*, 182 F.3d at 1238. Congress and the courts have historically viewed the opt-out regime as friendly to the free flow of information in a commercial marketplace, and the opt-in approach as creating barriers to entry. Symposium, *supra* note 17, at 29.

99 *See CPNI Order*, 13 FCC Rcd. at 8134, para. 95

plied customer approvals in the non-emergency context, however, raise privacy concerns that make the opt-out choice less desirable than the opt-in choice.[100]

While the meaning of "approval" in Section 222 offered at least two possible interpretations when the FCC promulgated its CPNI rules,[101] the meaning of "express prior authorization" in Section 222(f) is not ambiguous. The phrase does not connote "implied approval," as used in the E911 context, because of the word *express*.[102] Nor does the phrase suggest alternative opt-in/opt-out interpretations of the word *authorization* because of the inclusion of *express* and *prior*.[103] Taken together, Congress' choice of words in Section 222(f) suggests that "express prior authorization" means clear, unmistakable customer approval is required *before* using or disclosing location information relating to wireless subscribers.[104]

The challenge lies not in determining the meaning of "express prior authorization," but in determining an appropriate procedure for obtaining "express prior authorization." To delineate this requirement, Congress recently introduced the Wireless Privacy Protection Act of 2001 (H.R. 260), which proposes a specific notice and consent procedure for obtaining "express prior authorization" and requires the customer to furnish consent in writing.[105] The written consent requirement of this legislation may pose special problems for commercial location-based services. A court exercising judicial review over the written consent provision may find the requirement too restrictive to satisfy at least intermediate scrutiny under a First Amendment commercial speech challenge.[106]

("[N]otice and opt-out are likely to result in a greater percentage of implied 'approvals'."). Before the FCC shifted the balance between privacy and competition in the mid to late-1990s to make privacy a priority, as discussed earlier, it explicitly preempted most prior authorization rules that required an opt-in standard for CPNI use. *In re* Computer III Remand Proceedings: Bell Operating Company Safeguards and Tier 1 Local Exchange Company Safeguards, *Report and Order*, 6 FCC Rcd. 7571, 7636, para. 130 (1991). The FCC's rationale was that "[u]nder a prior authorization rule, a large majority of mass market customers are likely to have their CPNI restricted through inaction," thus vitiating a carrier's ability to achieve efficiencies by marketing integrated services to customers. *Id.* at 7610, para. 85 n.155.

100 *See* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 825 (2000) (stating that implied consent is a legal fiction that "neglects the actual conditions of choice regarding the processing of personal information"); EPIC Brief, *supra* note 46, at 14 (stating that an opt-out approach "would [place] an unreasonable burden on telephone customers to take additional steps to protect information that is, by all expectation, confidential"); Ann L. Lehman, *Email in the Workplace: A Question of Privacy, Property or Principle?*, 5 COMMLAW CONSPECTUS 99, 103 (1997) (stating that the idea of implied consent could work against an employee's claim of privacy if an employer provides notice that it monitors employee activities).

101 *See CPNI Order*, 13 FCC Rcd. at 8128, para. 87 ("We conclude that the term 'approval' in section 222(c)(1) is ambiguous because it could permit a variety of interpretations."). *But see U.S. West*, 182 F.3d at 1241 (Briscoe, J., dissenting) ("Although Congress did not specifically define the term 'approval' in the statute, its ordinary and natural meaning clearly 'implies knowledge and exercise of discretion after knowledge.'") (quoting BLACK'S LAW DICTIONARY 102 (6th ed. 1998)).

102 Black's Law Dictionary defines *express* in the following terms:

> Clear; definite; explicit; plain; direct; unmistakable; not dubious or ambiguous. Declared in terms; set forth in words. Directly and distinctly stated. Made known distinctly and explicitly, and not left to inference. Manifested by direct and appropriate language, as distinguished from that which is inferred from conduct. The word is usually contrasted with 'implied.'

BLACK'S LAW DICTIONARY 402 (6th ed. 1998).

103 Black's Law Dictionary defines *prior* as "[e]arlier; elder; preceding; superior in rank, right, or time." *Id.* at 1193.

104 As a precedent to retrieving "express prior authorization," FTC guidelines suggest that carriers should provide notice of the type information that it collects; how it collects the information; persons or third parties that have access to the information; and, how it uses the information in order for the customer's authorization to constitute adequate consideration for the carrier's data collection activities. These guidelines for obtaining notice follow the FTC's description of "Notice" as set forth in its Fair Information Practices for the Electronic Marketplace. *See* FTC REPORT TO CONGRESS, *supra* note 93, at iii.

105 Wireless Privacy Protection Act of 2001, H.R. 260, 107th Cong. (2001). H.R. 260 proposes to amend Section 222 to clarify the procedure for obtaining "express prior authorization" required by Section 222(f). The consent must include a description of the specific types of information collected by the carrier, how the carrier uses the information, and what information it shares or sells to third parties. H.R. 260 at § (2)(a).

106 Courts now analyze First Amendment commercial speech challenges under an intermediate level of scrutiny according to the *Central Hudson* test. *Cent. Hudson Gas & Elec. Corp.*, 447 U.S. at 566. Recently, however, it has been observed that the Supreme Court believes that intermediate scrutiny may not provide adequate protection for a company's marketing and advertising activities. *See* Lorillard Tobacco Co. v. Reilly, 218 F.3d 30, 42–43 (1st Cir. 2000), *cert. granted*, 531 U.S. 1068 (2001) ("In declining to impose a more searching review than that mandated by *Central Hudson*, we are aware of the recent rumblings from members of the Supreme Court and others suggesting that the *Central Hudson* test may be in need of minor or major modification."); Linda Greenhouse, *Justices to Hear Challenge to Cigarette Ad Restrictions*, N.Y. TIMES, Jan. 9, 2001, at A16 ("The [C]ourt has grown increasingly protective of commercial

By contrast, the FCC and industry groups have offered more flexible approval procedures for gaining customer authorization for using CPNI in location-determining technology. In drafting its CPNI Order, the FCC dismissed a written-only consent requirement as inconvenient for both the customer and the carrier. The FCC instead allowed written, oral or electronic approval of CPNI use and disclosure.[107] In a November 2000 filing with the FCC, the Cellular Telecommunications Industry Association suggested that customers provide "express prior authorization" for location information use and disclosure through written, oral or electronic means.[108]

The choice between written, oral or electronic authorization methods accommodate practical considerations for wireless location information services more adequately than a written-only requirement. The traditional method for obtaining customer consent is having the customer sign a service agreement that provides comprehensive details of the carrier's location information practices prior to beginning service.[109] Some wireless subscribers, however, may prefer using à la carte location services on an infrequent basis, rather than committing to comprehensive and more costly location service plans that are always in use. To give these customers the option to retrieve, on occasion, navigational instruction while driving motor vehicles in an unfamiliar city, customers may prefer to provide oral or electronic consent for single service transactions through a mobile phone or PDA. As discussed below, the screen size of most mobile phones and PDAs provides its own challenges in communicating a complete and accurate privacy policy to which customers can offer their "express prior authorization."[110] But once a customer understands her privacy rights, she could provide either oral consent by speaking to her carrier's customer service personnel over her wireless phone or electronic consent by pushing a designated button on her PDA.[111] Ultimately, when customers provide their "express prior authorization," they should understand accurately to how such personal information will be used.[112]

---

speech in the past 20 years, and in recent cases most of the current justices have indicated in one way or another that the *Central Hudson* test is inadequate.").

107 *CPNI Order*, 13 FCC Rcd. at 8131, para. 92 (noting that "oral approval promotes customer and carrier convenience," and that "Congress sought to facilitate that").

108 *CTIA Petition*, *supra* note 13, at 9. CTIA suggested the FCC adopt four privacy principles modeled after the FTC's Fair Information Practices. First, providers must inform customers about personal information collection and use practices before disclosure of location information occurs. Second, customers must provide "express prior authorization" through written, oral or electronic means. Third, location service providers should protect the location information from unauthorized access and disclosure to third parties. Fourth, the notice, consent and security privacy standards should be technology neutral so that standards remain the same whether the service is handset or network-based. *Id.* at 9–11.

109 Incorporating privacy disclosures in already lengthy and complex service agreements may be an insufficient method of obtaining meaningful user consent. *See* Stefanie Olsen, *Earthlink Promises "Anonymous" Web Surfing*, CNET NEWS.COM, *at* http://news.cnet.com/news/0-1005-200-5068930.html (Mar. 8, 2001) [hereinafter Olsen, *Earthlink Promises*] (noting that "consumers are largely clueless when it comes to details because of the complexity of standard privacy policies," and burying the terms in lengthy user agreements may render disclosure ineffective).

110 *See* Meta Group, *Commentary: Java Has No Future on Cell Phones*, CNET NEWS.COM, *at* http://news.cnet.com/news/0-1003-200-2816353.html (Sept. 19, 2000) (indicating that despite cell phone manufacturer experiments with high-tech answers to "the tiny-screen problem," most technologies remain too expensive to be practical).

111 OnStar, a provider of location-based navigational services installed in many popular automobiles, states that it relays location information to service personnel only after the subscriber provides either a correct Personal Identification Number or Security Word, which are presumably either spoken through a voice system or entered electronically using a keypad. *See* ABOUT ONSTAR: FREQUENTLY ASKED QUESTIONS, *at* http://www.onstar.com/visitors/html/ao_faq.htm#privacy (last visited Sept. 1, 2001). Cell phone manufacturers are developing technology to make typing text messages more manageable. The more manageable that cell phone keypads become, the more practical it will be for location service customers to enter user IDs, passwords and other information that may constitute electronic consent. *See* Ben Charny, *Software Makes Cell Phone Typing Easier*, CNET NEWS.COM, *at* http://news.cnet.com/news/0-1004-202-4722626-0.html (Feb. 6, 2001) (noting that "it's incredibly difficult, time-consuming and frustrating to type text on a cell phone dial pad").

112 *See* FEDERAL TRADE COMMISSION, *In re* International Outsourcing Group, Inc., *at* http://www.ftc.gov/os/2000/07/iogchair.htm (July 12, 2001) (Statement of Chairman Robert Pitofsky and Commissioner Mozelle Thompson) (justifying the scope of injunctive relief relating to defendant's misrepresentation that information collected from website users would be used only for medical consultation and billing, when the information was used to develop a targeted marketing list and disclosed to third parties). CTIA suggests that consent for particular transactions should extend only to the life of that transaction and should "not authorize any other use or disclosure without further approval by the customer." *CTIA Petition*, *supra* note 13, at 10 n.24.

III. BEYOND TITLE II: PRIVACY RULES AND POLICIES FOR NON-CARRIERS

Carriers will likely serve as the gatekeepers of location information due to their investment in position-determining technology and because Section 222 mandates that carriers not disclose CPNI without the customer's express prior authorization. Therefore, carriers are unlikely to disclose location information to non-carrier application and content providers unless those third parties have adopted and enforced their own set of principles for protecting consumer privacy. As an initial matter, non-carrier application providers and content developers are not governed by Title II of the Communications Act and thus are not subject to Section 222 CPNI restrictions.[113] Non-carriers that collect, use, sell or otherwise distribute personally identifiable information, however, have no less interest in promoting privacy policies and practices that further market acceptance of the location services industry.[114] When a carrier obtains express prior authorization for disclosure of consumers' personal information to third party providers, location privacy becomes the responsibility of those third parties.[115]

A. Fair Information Practices for the Electronic Marketplace

1. Privacy Policies: "Clear and Conspicuous" Notice

Consumer advocates and federal regulators have urged commercial website operators that collect information about their users to post prominent privacy policies that clearly disclose collection and use practices for consumer's personal information.[116] The Federal Trade Commission has stated that such privacy notices should be "clear and conspicuous" and include: what information is being collected; its intended uses; the third parties to whom it will be disclosed; the consumer's ability to gain access to the information; and the consumer's ability to remove information from the company's database.[117] The 2000 Georgetown Internet Privacy Policy Survey Report found that 62% of websites in a random sample of websites with more than 39,000 unique monthly visitors and 97% of the most popular sites on the web posted a privacy policy of some sort.[118] These figures indicate that privacy notices have become a common practice on the web and will likely play an important role for the location services indus-

---

113 Title II of the Communications Act of 1934, entitled "Common Carriers," stipulates certain rules for providers that qualify as telecommunications carriers. The Communications Act defines "telecommunications carrier" as "any provider of telecommunications services." 47 U.S.C. § 153(44). The Communications Act defines "telecommunications service" as "the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used." 47 U.S.C. § 153(46). *See generally* BRANDS & LEO, *supra* note 42, at 109–51.

114 *See* FEDERAL TRADE COMMISSION, *In re* ReverseAuction.com, *at* http://www.ftc.gov/os/2000/01/reversemt.htm (Jan. 6, 2001) (Statement of Commissioner Mozelle Thompson) (noting that breaching the privacy expectations of consumers undermines consumer confidence and "diminishes the electronic marketplace for all its participants").

115 *See* Raul, *supra* note 35 ("Although telecom carriers are prohibited by law from divulging their customers' locations except to police, other [PSAPS], and (in certain cases) family members, wireless telecom carriers and other mobile device providers are certainly allowed to use or resell the data with customers' consent.").

116 *See* FEDERAL TRADE COMMISSION, STIPULATED FINAL ORDER FOR PERMANENT INJUNCTION, FTC v. RENNERT 4, *at* http://www.ftc.gov/os/2000/07/iogstipmort.htm (July 12, 2000) [hereinafter RENNERT ORDER] (ordering defendant website operator to "provide notice to consumers of its practices with regard to its collection and use of personal information"); FEDERAL TRADE COMMISSION, AGREEMENT CONTAINING CONSENT ORDER, *In re* Geocities 3, *at* http://www.ftc.gov/os/1998/9808/geo-ord.htm (Aug. 13, 1998) [hereinafter GEOCITIES CONSENT ORDER] (ordering defendant website operator to provide "clear and prominent notice" with respect to defendant's practices regarding its collection and use of personal identifying information); BETTER BUSINESS BUREAU, BBBONLINE, CODE OF ONLINE BUSINESS PRACTICES 13, *at* http://www.bbbonline.com/code/code.asp (last visited Sept. 1, 2001) (stating that online advertisers should provide "notice as to what personal information the online advertiser collects, uses, and discloses").

117 GEOCITIES CONSENT ORDER, at 3; FEDERAL TRADE COMMISSION, AGREEMENT CONTAINING CONSENT ORDER, *supra* note 116 *In re* Liberty Financial Companies 4, *at* http://www.ftc.gov/os/1999/9905/lbtyord.htm (May 6, 1999) [hereinafter LIBERTY FINANCIAL CONSENT ORDER]; FTC REPORT TO CONGRESS, *supra* note 93, at 14.

118 FTC REPORT TO CONGRESS, *supra* note 93, at 10. "Unique visitors" refers to different individuals that visited a website in a monthly period without regard to how long they spent at the website or how many times they returned. *Id.* at 45. The "most popular websites" included the 100 busiest sites on the web. *Id.* at 7. The FTC indicated, however, that websites received credit for "Notice" if it posted a privacy policy that identified at least one specific type of information that it collected and at least one use to which the information will be put. This methodology leaves open the possibility that websites are collecting, using and disclosing more than they claim. *Id.* at 23.

try as well. The FTC has stated, "[t]he Notice principle is the most fundamental of the fair information practice principles, because it is a prerequisite to implementing other fair information practice principles."[119]

As with carrier procedures for obtaining "express prior authorization," providing a "clear and conspicuous" privacy notice presents unique challenges for the location services industry due to the limiting physical characteristics of the devices to which services will be delivered. Third Generation ("3G") mobile phones may come packaged as handheld computers capable of making phone calls, sending email, broadcasting movies, playing video games and taking digital photographs.[120] It is difficult, however, to imagine location service customers effectively reading through a comprehensive privacy policy presented on a small screen.[121] Although a handheld PC or other PDA may offer slightly larger screen space to deliver privacy notices, these devices are currently incapable of handling the wireless download of large documents.[122]

Restricting the disclosure of information collection and use practices in order to accommodate the limited document delivery and retrieval capabilities of wireless devices would inevitably raise questions concerning whether adequate notice has been provided to consumers. One solution for the notice problem may require that customers review and agree to a provider's complete privacy policy provided either online, using a desktop or laptop PC for retrieval and review, or on paper.[123] An abbreviated notice of the privacy policy would then be available to the customer through the wireless device, accompanied by instructions on how customers may retrieve and review the full policy.[124] Or a provider could offer audio messages relayed through a mobile phone that describe fully its information practices and the customer's privacy rights.[125]

Regardless of how privacy policies are implemented, location service providers will be bound to the terms and conditions stated in their privacy notices and should expect the FTC to examine closely any alleged violations of these policies. The Federal Trade Commission Act ("FTC Act")[126] empowers the FTC to prevent persons, partnerships or corporations from using "unfair or deceptive acts or practices in or affecting commerce."[127] The FTC commenced five major actions against different website operators in the last decade and accused them of conducting deceptive or unfair acts or practices in violation of the FTC Act.[128] The FTC alleged that the defendants

---

119 *Id.* at 14.

120 Regan Morris, *Asia Seeks Wireless Web Phone Lead*, ASSOCIATED PRESS, Feb. 25, 2001, *available at* WL 13676755. Third generation ("3G") wireless systems "could provide . . . a wide range of voice, data and broadband services over a variety of mobile and fixed networks." *In re* Amendment of Part 2 of the Commission's Rules to Allocate Spectrum Below 3GHz for Mobile and Fixed Services to Support the Introduction of New Advanced Wireless Services, Including Third Generation Wireless Systems, *Notice of Proposed Rulemaking and Order*, 16 FCC Rcd. 596, para. 1 (2001). The FCC has initiated action allocating additional spectrum to meet the increasing needs of wireless providers in the United States and elsewhere that have begun to offer mobile data services, such as electronic mail, Internet access and short messaging service. *Id.* at para. 12.

121 Meta Group, *Commentary: Can PDAs Fill Corporate Needs?*, CNET NEWS.COM, *at* http://news.cnet.com/news/0-1006-200-4118021.html (Dec. 12, 2000) ("Despite more powerful processors, the devices will always be limited by the needs of the human interface; small screen size, in particular, will always limit their usefulness.").

122 *See id.* ("Although PDAs could prove useful for wireless, automated notifications from enterprise resource planning (ERP) systems—and they can also be useful for short emails—they are not capable of handling the large attachments that are becoming increasingly common elements of corporate email.").

123 CTIA suggests that service providers inform customers about their location information practices either through a service agreement prior to the commencement of service, through an electronic mail message, on a website, or in a letter sent to subscribers. *CTIA Petition*, *supra* note 13, at 9.

124 *See id.* ("Consumers could also get notice on a bill directing subscribers to a toll-free number or Internet site address for a description of the carrier's complete policies and practices.").

125 Some Internet retailers have begun offering audio recordings of their privacy policies through their websites in an effort to cultivate customer relationships. *See* Stefanie Olsen, *E-tailers Give New Voice to Customer Service*, CNET NEWS.COM, *at* http://news.cnet.com/news/0-1007-200-3942079.html (Dec. 1, 2000).

126 15 U.S.C. §§ 41 *et seq.* (1994 & Supp. V 1999). The FTC's authority over the collection and dissemination of personal information collected by electronic service providers is derived from Section 5 of the FTC Act and the Children's Online Privacy Protection Act ("COPPA"). 15 U.S.C. § 45(a) (1994 & Supp. V 1999); 15 U.S.C. §§ 6501 *et seq.* (Supp. V 1999). COPPA was passed by Congress in October 1998 and required the FTC to promulgate rules concerning children's online privacy. Under COPPA, operators of websites targeted to children must post clear and comprehensive privacy policies describing their information practices, obtain parental consent before collecting information from children, and meet other requirements.

127 15 U.S.C. § 45(a)(1).

128 *See* FEDERAL TRADE COMMISSION, FIRST AMENDED COM-

used personal information[129] obtained through the Internet contrary to how consumers expected that information would be used.[130] In each case, defendants signed consent agreements with the FTC and promised to abide by clear and conspicuous privacy policies that accurately and completely described their information use, collection and distribution practices.[131]

2. *Choice: Non-carrier Adoption of "Express Prior Authorization"*

Beyond providing notice of information practices, under the FTC rules "Choice" involves the opt-in/opt-out debate discussed above and is a key factor for consumers controlling access to their personal information.[132] One survey has estimated that 88% of Internet users always want websites to ask permission before sharing their personal information with others.[133] This suggests that non-carrier providers in the location services industry should adopt the "express prior authorization" standard of Section 222 and implement opt-in consent mechanisms for "Choice" in order to attract and retain the widest number of wireless customers.

Providers may explore a variety of methods to obtain a customer's opt-in consent for using his or her personal information. CTIA suggests that "[c]onsent may be express yet implicit" in certain transactions, as when a wireless subscriber calls a service for driving directions.[134] In these situations, CTIA suggests that the caller's act of requesting the service satisfies the consent requirement, albeit implicitly.[135] CTIA compares this consent to the implied consent standard for 911 emergency calls made by wireless customers.[136] Rather than blurring the line between emergency transactions and some commercial transactions where implied consent is allowed, customer privacy may be better protected if carriers always offer the customer an opportunity to provide at least oral or electronic consent when service requests are made. The fact that an overwhelming majority of Internet users repeatedly emphasize a desire to give express permission before a website collects personal information indicates that allowing implied consent for commercial location

PLAINT FOR PERMANENT INJUNCTION AND OTHER EQUITABLE RELIEF, FTC v. TOYSMART.COM, *at* http://www.ftc.gov/os/2000/07/toysmartcomplaint.htm (July 21, 2000) [hereinafter Toysmart Complaint] (alleging that defendant solicited bids for the purchase of personal information collected from its website contrary to its stated privacy notice); FEDERAL TRADE COMMISSION, COMPLAINT FOR PERMANENT INJUNCTION AND OTHER EQUITABLE RELIEF, FTC v. REVERSEAUCTION.COM, *at* http://www.ftc.gov/os/2000/01/reversecmp.htm (Jan. 6, 2000) [hereinafter REVERSEAUCTION.COM COMPLAINT] (alleging that defendant violated the terms and conditions of a competitor's user agreement by harvesting customer information from the competitor's website and using it to send unsolicited email messages); FEDERAL TRADE COMMISSION, COMPLAINT FOR PERMANENT INJUNCTION AND OTHER EQUITABLE RELIEF, FTC v. RENNERT, *at* http://www.ftc.gov/os/2000/07/iogcomp.htm (July 12, 2000) [hereinafter RENNERT COMPLAINT] (alleging that defendant falsely represented to website customers that their personal information would be protected by encryption and other technologies); FEDERAL TRADE COMMISSION, COMPLAINT, *In re* Liberty Financial Companies, *at* http://www.ftc.gov/os/1999/9905/lbrtycmp.htm (May 11, 1999) [hereinafter LIBERTY FINANCIAL COMPLAINT] (alleging that defendant website operator misrepresented that the identity of website users who registered to participate in an online survey would remain anonymous); FEDERAL TRADE COMMISSION, COMPLAINT, *In re* Geocities, *at* http://www.ftc.gov/os/1998/9808/geo-cmpl.htm (Apr. 28, 1998) [hereinafter GEOCITIES COMPLAINT] (alleging that defendant sold, rented or otherwise disclosed customer's personal information to third parties contrary to its privacy policy).

129 As used by the FTC, personal information generally refers to individually identifiable information about a person and includes name, address, email address, telephone number, social security number and other information about a user that a website operator gathers online. *See* RENNERT ORDER, *supra* note 116, at 2–3.

130 TOYSMART COMPLAINT, *supra* note 128; REVERSEAUCTION.COM COMPLAINT, *supra* note 128; RENNERT COMPLAINT, *supra* note 128; LIBERTY FINANCIAL COMPLAINT, *supra* note 128; GEOCITIES COMPLAINT, *supra* note 128.

131 GEOCITIES CONSENT ORDER, *supra* note 116; RENNERT ORDER, *supra* note 116; LIBERTY FINANCIAL CONSENT ORDER, *supra* note 117; FEDERAL TRADE COMMISSION, STIPULATED CONSENT AGREEMENT AND FINAL ORDER, *In re* ReverseAuction.com, *at* http://www.ftc.gov/os/2000/01/reverseconsent.htm (Jan. 6, 2000) [hereinafter REVERSEAUCTION.COM ORDER]; FEDERAL TRADE COMMISSION, STIPULATED CONSENT AGREEMENT AND FINAL ORDER, FTC v. TOYSMART.COM, *at* http://www.ftc.gov/os/2000/07/toysmartconsent.htm (July 21, 2000) [hereinafter TOYSMART Order].

132 In the web environment, the FTC has reported that consumers are extremely concerned about whether websites will share their personal information with third parties. One survey cited by the FTC revealed that 92% of Internet users would be uncomfortable if a website shared their information with other entities. FTC REPORT TO CONGRESS, *supra* note 92, at 15 (citing a Business Week/Harris Poll, *A Growing Threat*, Mar. 20, 2000, *available at* http://www.businessweek.com/2000/00_12/b3673010.htm?scriptFramed).

133 *Id.*

134 *CTIA Petition*, *supra* note 13, at 10 n.24.

135 CTIA adds that implied consent "extends only to the use of location information for that particular transaction and would not authorize any use or disclosure without further approval by the customer." *Id.*

136 *Id.*

services could have devastating effects on a new technology that questions widely held privacy beliefs.[137]

3. *Access: Giving Customers a "Behind the Scenes" View*

While "Notice" and "Choice" may be straightforward principles commonly accepted in the electronic marketplace,[138] the practice of allowing customers the opportunity to access, view, change, and delete information collected and stored about them raises its own implementation issues.[139] In the past, the FTC has required website operators in violation of the FTC Act to disclose in their privacy notices information about the consumer's ability to obtain access to personal information collected through their websites.[140] These requirements demand that the website operator indicate whether consumers will have access to personally identifiable information gathered about them but do not actually require website operators to provide access. Although the FTC has proposed various models for implementing Access, it has not offered a definitive standard suggesting how consumers should gain "reasonable access" to information stored about them.[141]

The FTC is only beginning to address Access issues on the web. Nonetheless, it has recognized that wireless location services pose unique privacy challenges because of the fact that consumers may not know exactly what providers are doing with information about *where* they are online, and what they are doing there.[142] The FTC insists that private industry will derive value from including consumers in the process of collecting information by ensuring that consumers are aware of what information providers are gathering about them.[143] This advice suggests that supplying notice of information collection and storage activities may be enough to keep customers involved in the process. Privacy advocates, however, claim that allowing consumers to have a "behind the scenes" view of how their information is handled goes hand in hand with the validity of privacy notices.[144]

As location service providers develop technologies for offering their products to a mass audi-

---

137 FTC REPORT TO CONGRESS, *supra* note 92, at 15.

138 *See* Olsen, *Earthlink Promises*, *supra* note 109 (noting that most major Internet Service Providers have "reasonable privacy policies that reassure consumers that they're not doing anything untoward with their customer data").

139 FTC REPORT TO CONGRESS, *supra* note 92, at 29 (stating that the implementation of Access is a complex task surrounded by industry disagreement as to how Access should be provided). An FTC advisory committee has identified major problems involving implementation of Access relating to the scope of information to which consumers should have access; the entities that should be obligated to provide consumers access to information about them; and, the appropriate and feasible means to authenticate access requests to prevent unauthorized access. *Id.* The FTC established the Advisory Committee on Online Access and Security "to consider the parameters of 'reasonable access' to personal information collected from and about consumers online and 'adequate security' for such information." *Id.* at 28.

140 GEOCITIES CONSENT ORDER, *supra* note 116, at 3 (requiring the defendant to include in its privacy policy information about "the consumer's ability to obtain access to or directly access [personal information collected by defendant's website] and the means by which (s)he may do so"); REVERSEAUCTION.COM ORDER, *supra* note 131 (requiring the defendant to include in its privacy policy information about the customer's ability to obtain access to his or her own personal information collected by the defendant); RENNERT ORDER, *supra* note 116, at 5 (requiring defendant to disclose "[the] means by which a consumer may access and review personal information concerning him or her" and "[the] means by which a consumer may modify . . . or delete personal information, concerning him or her").

141 The FTC has suggested four options for implementing Access. Under a "total access approach," a consumer can access all information "regardless of medium, method or source of collection, or the type of data in question." FTC REPORT TO CONGRESS, *supra* note 92, at 29–30. A "default to consumer access" approach allows website operators to classify information as either "retrievable in the ordinary course of business," which consumers can retrieve by following a regular procedure, or as an "unreasonable burden," which is not retrievable in the ordinary course of business. Under the "case-by-case" approach, access depends on the content, holder, source and likely use of the information. The "access for correction" approach allows a website operator to grant access to personal information stored in its databases only when the information is used to grant or deny significant benefits to the consumer, such as financial, credit or medical benefits. *Id.* at 30–31. Without specifying a preferred option, the FTC stated that it "believes that all of these implementation options will be useful to Web sites in developing procedures to facilitate consumer access to personal information collected from and about them, and that the options will be relevant to any determination as to the scope of 'reasonable access'." *Id.* at 31.

142 *FTC Forum Targets Privacy, Security of Wireless Internet*, TELECOMMS. REPS., Jan. 8, 2001, at 28.

143 *Id.*

144 Olsen, *Earthlink Promises*, *supra* note 109. A recent survey of Canadian Internet users revealed that 55% of respondents would be willing to provide personal information to an online billing service if they had the ability to remove their name and information from the service's database. *Deriven-Commissioned Research Confirms Privacy is a Key Issue Influencing Consumer Acceptance of Internet Billing*, PR NEWSWIRE, Jan. 16, 2001.

ence, implementing an Access mechanism would enhance customer involvement and increase the value of the contemplated service. For example, an application provider is likely to store information about a customer that it has learned from the customer's responses to a questionnaire or from the customer's usage habits and/or service requests.[145] As part of a service agreement with the customer, the provider could offer access to a website that allows the customer to log in and retrieve details of her profile as if she were retrieving information about deposits and withdrawals in an online banking system. An additional privacy feature advocated by the FTC would allow the customer to delete, modify, or correct information, and to view the names of any third parties with whom the provider has shared the customer's personal information.[146]

4. Security: Interception and Surveillance

As arguably the most important principle, Security is a technical matter that underlies the privacy effects of Notice, Choice and Access.[147] While this comment cannot adequately cover the technical issues behind protecting electronic information from unauthorized access and abuse, two points regarding security merit discussion here.[148] First, the Electronic Communications Privacy Act makes it a crime to intercept any wire, oral or electronic communication.[149] Location information appears to fall under the ECPA's definition of "electronic communication," which includes any data transmitted by radio.[150] Thus, the ECPA should prohibit application and content providers from intercepting location information to deliver services when the carrier refuses to disclose such data. The definition of "electronic communication," however, excludes "any communication from a tracking device"[151] and considers "tracking device" to mean "an electronic or mechanical device which permits the tracking of the movement of a person or object."[152] Wireless devices equipped to monitor the movement of a user so that the user can receive time-sensitive and location-based marketing messages conceivably fall under the protection of the "tracking device" exception.[153]

Although many of the principles advocated in this comment can be implemented by the affected industries as self-regulatory changes, congressional action amending the definition of "tracking

145 Rachel Konrad, *General Motors to "Push" Ads to Drivers*, CNET NEWS.COM, *at* http://news.cnet.com/news/0-1005-200-4408227.html (Jan. 8, 2001) [hereinafter Konrad]. General Motors is testing location-based advertising that sends commercial messages to drivers who have signed up for the program and completed a "confidential questionnaire" indicating the type of advertisements they would like to receive. *Id.*

146 FTC REPORT TO CONGRESS, *supra* note 92, at iii.

147 The FTC "Security" policy is that website operators should "take reasonable steps to protect the security of the information they collect from consumers." *Id.* at 37.

148 *See* FEDERAL TRADE COMMISSION, FTC WORKSHOP: THE MOBILE WIRELESS WEB, DATA SERVICES, AND BEYOND: EMERGING TECHNOLOGY AND CONSUMER ISSUES, RESPONSE STATEMENT OF GREGORY A. MILLER FOR DAY II PANEL: BUILDING PRIVACY AND SECURITY SOLUTIONS INTO THE TECHNOLOGICAL ARCHITECTURE, *at* http://www.ftc.gov/bcp/workshops/wireless/comments/miller.pdf (Dec. 11, 2000) (describing specific security features to ensure customer privacy in the wireless environment, including encryption, pseudonymity and open platform devices that allow users to load their own security technologies).

149 Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2520 (1994 & Supp. V 1999). Section 2511 of the ECPA states that any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral or electronic communication;" or "intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication" is subject to criminal and civil penalties described in the statute. 18 U.S.C. § 2511(1) (1994). For an analysis of the ECPA prohibitions against interception of wire, oral or electronic communications, *see* HARVEY L. ZUCKMAN ET AL., MODERN COMMUNICATION LAW, 858–70 (1999). Section 605 of the Communications Act of 1934 complements the ECPA by requiring that "no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof" to unauthorized sources. 47 U.S.C. § 605(a) (1994).

150 18 U.S.C. § 2510(12). Under the ECPA "electronic communication" means

> any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include— (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

Id. at § 2510(12).

151 18 U.S.C. § 2510(12)(C).

152 18 U.S.C. § 3117(b) (1994).

153 *See* Hawkins, *supra* note 30, at 74 (noting that cell phones are becoming tracking devices to which retailers send marketing messages based on the user's location).

device" may help safeguard privacy and allay security concerns related to interception in the location services industry. Additional language in the ECPA suggests that "tracking device" refers to court-ordered instruments installed by law enforcement officials to monitor criminal activities. The definition itself falls among statutory provisions governing searches and seizures.[154] Legislation further clarifying the contextual definition of "tracking device" would ensure that anyone who wrongfully obtained location information and abused personal privacy could not hide under the tracking device exception found in the ECPA.

A second security issue deserving attention is whether wireless phones will become tracking devices for location-based marketing, thereby raising questions over surveillance.[155] The delivery of location services will be based on either a "push" or "pull" model. Customers will trigger "pull" services when they request navigational directions, yellow page directories and/or weather from a location service provider. A service provider will "push" location-based coupons or other time-sensitive notifications to a passive customer based on the customer's geographical positioning. The "push" model requires the location service provider to conduct surveillance on its customers in order to determine when customers should receive certain messages and notices. To privacy advocates, surveillance through devices equipped to work with location-tracking technologies raises the specter of "Big Brother" in the wireless industry.[156] To eliminate this problem, wireless subscribers have the ability to turn their devices off, thereby turning off location-monitoring systems that track their movements. As a more practical solution, service providers could offer customers a way to deactivate commercial location-monitoring systems even when their wireless devices remain active for other services, including E911 access.

B. Other Lessons from the Web: Profiling, Spam, Self-Regulation and Legislation

1. Location-Based Profiling: An Experiment in Self-Regulation

Profiling is the major business application of many location service providers and immediately raises concerns among privacy advocates.[157] In a recent report to Congress, the FTC described profiling as activities in the electronic marketplace that match the Internet usage habits of consumers with personally identifiable information and, in some cases, combine these profiles with data obtained through consumers' offline purchases, surveys and registration forms.[158] The result of combining online and offline data "is a detailed profile that attempts to predict the individual consumer's tastes, needs, and purchasing habits and enables the advertising companies' computers to make split-second decisions about how to deliver ads directly targeted to the consumers' specific interests."[159] If added to such profiles, location information enhances the value of profiling activities by contributing details of individuals' geographical position.[160]

Profiling activities on the web are governed by

---

154 The definition of "tracking device" is provided in a part of Title 18 that covers search and seizure by law enforcement officials. 18 U.S.C. § 3117. Generally, "[I]f a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction." 18 U.S.C. § 3117(a). This general provision is followed by the definition for "tracking device" in § 3117(b).

155 The constitutionality of GPS-based surveillance by law enforcement officials has come before courts in a few cases. *See* United States v. McIver, 186 F.3d 1119 (9th Cir. 1999); United States v. Nerber, 222 F.3d 597 (9th Cir. 2000). These decisions have little impact on the broader location services industry beyond noting that surveillance embodies privacy concerns. Daniel R. Sovocool, *GPS Tracking Case Raises Privacy Issues*, *at* http://www.thelenreid.com/articles/article/art_61.htm (last visited Sept. 1, 2001).

156 Lisa M. Bowman, *Gadgets Play Role of Big Brother*, CNET NEWS.COM, *at* http://news.cnet.com/news/0-1005-200-5067281.html (Mar. 8, 2001); John Borland, *Wireless Phone Tracking Plans Raise Privacy Hackles*, CNET NEWS.COM, *at* http://news.cnet.com/news/0-1004-200-3624256.html (Nov. 10, 2000).

157 *See* Hon. William D. Daley, Secretary of Commerce, Remarks at the Public Workshop on Online Profiling (Nov. 8, 1999) *available at* http://www.ftc.gov/bcb/profiling/online.pdf.

158 FEDERAL TRADE COMMISSION, ONLINE PROFILING PART 2: RECOMMENDATIONS 3, *at* http://www.ftc.gov/os/2000/07/onlineprofiling.pdf (July 2000) [hereinafter FTC PROFILING RECOMMENDATIONS].

159 *Id.*

160 *See* Jeff Sweat, *The Well-Rounded Consumer: Companies Must Strive for a Complete View of Their Customers as the Relationship Shifts from Commerce to Collaboration*, INFORMATIONWEEK, Apr. 10, 2000. General Motors "has integrated . . . financial information, purchase history, vehicle information, and service records in a single system, all connected to its Web site. Now it's working on tighter integration to the data it collects from the OnStar system." *Id.*

industry self-regulation in the United States. Under self-regulation, industry is presumably motivated to protect consumer privacy out of a fear of either bad publicity, or a backlash from consumers who simply do not accept industry's disregard for personal privacy.[161] The FTC initially encouraged industry to address consumer privacy concerns on the web through self-regulation.[162] When it noted that a vast majority of websites failed to implement self-regulatory principles and that enforcement was nonexistent, the FTC reversed itself and asked Congress to enact legislation that would "set forth a basic level of privacy protection for all visitors to consumer-oriented commercial Web sites" not already covered by the Children's Online Privacy and Protection Act.[163] Included in this request was "backstop legislation addressing online profiling."[164] Many scholars have also concluded, as did the FTC, that self-regulation on the Internet has been unsuccessful in protecting consumer privacy.[165]

Despite current attitudes toward self-regulation, the location service industry has the opportunity to represent a model of effective self-regulation for privacy practices in the electronic marketplace. A legislative approach is unappealing at this point for several reasons. The location services industry is distinctly different from other electronic industries due to its unique technology and innovative business models. Legislators have much information about Internet technologies and business practices, but the fundamental characteristics of the location services industry are still largely unknown. Because of these differences, it would be inappropriate to extend rules for the current online industry to practices in the nascent location services industry.

Drafting new legislation for the location services industry promises both heavy expenditures and regulatory inflexibility.[166] Taxpayers will bear the heavy administrative costs of drafting, administering and enforcing any new privacy rules.[167] Rules are difficult to change, and rapid technological and market developments for the location services industry demand flexibility.[168] H.R. 260, discussed earlier in Part Two of this comment demonstrates how legislation may be too inflexible to accommodate technological innovation.[169] H.R. 260 does not consider future technological developments that could make oral or electronic authorization efficient and even preferred methods for acquiring "express prior authorization." As an additional matter, legislative proposals like H.R. 260 could create an incentive for the location services industry to avoid seeking self-regulatory solutions.[170]

By addressing privacy concerns now, location service providers can overcome the major limitations inherent in self-regulation and provide a better example of self-regulation than their Internet counterparts. The major limitations of self-regulation are the inability of consumers to gain information about a company's privacy policy and the failure to ensure that the company enforces its privacy policy.[171] Location service providers can address these concerns by implementing the

---

161 Scott Foster, *Online Profiling is on the Rise: How Long Until the United States and the European Union Lose Patience with Self-Regulation?*, 41 SANTA CLARA L. REV. 255, 266–67 (2000) [hereinafter Foster]; Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, U.S. Dep't of Commerce, A Report to the Nat'l Telecomm. and Info. Admin. (Sept. 8, 1997) [hereinafter Swire] ("[T]he incentives for industry to protect privacy are entirely financial").

162 FTC REPORT TO CONGRESS, *supra* note 92, at 35. According to the FTC, effective self-regulation in the Internet industry required businesses to adopt and implement at least the Notice and Choice prongs of its four Fair Information Practices as well as an efficient enforcement mechanism to govern self-regulatory programs. *Id.* at 34–35. The FTC also found that self-regulatory seal programs such as TRUSTe and BBBOnline, which issue seals to websites complying with their programs' privacy principles, were used by only 8% of heavily-trafficked websites it examined. *Id.* at 35; *see also* Foster, *supra* note 161, at 271–72.

163 FTC REPORT TO CONGRESS, *supra* note 92, at 36; *see* COPPA, *supra* note 126 and text accompanying note 126 (discussing the Children's Online Privacy Protection Act); FTC PROFILING RECOMMENDATIONS, *supra* note 158, at 10.

164 FTC Profiling Recommendations, *supra* note 158, at 10 ("Self-regulation cannot address recalcitrant and bad actors, new entrants to the market, and drop-outs from the self-regulatory program.").

165 Foster, *supra* note 161, at 275; FTC REPORT TO CONGRESS, *supra* note 92, at 36.

166 Swire, *supra* note 161.

167 *Id.*

168 *Id.*; *see* FTC PROFILING RECOMMENDATIONS (dissenting statement of Commissioner Swindle), *supra* note 158 (noting that legislation that mandates the four fair information practice principles on an entire industry is overly burdensome because of differences within the industry among some advertisers adopting a self-regulatory approach, and others to whom the principles may not apply).

169 H.R. 260.

170 FTC PROFILING RECOMMENDATIONS (dissenting statement of Commissioner Swindle), *supra* note 158.

171 Swire, *supra* note 161; FTC REPORT TO CONGRESS, *supra* note 92, at 34–35.

Notice principle found in the FTC's fair information practices. Any violation of its own Notice provision would subject a company not only to action under the FTC Act, but also to consumer backlash.[172] In addition, seal programs for the location service industry like those now in operation on the Internet could allow providers to display their credentials as users of accepted location privacy principles.[173] It is conceivable that consumers may be willing to forsake some privacy to benefit from targeted location-based advertising reflecting their preferences for stores and restaurants.[174] Legislators may not now recognize the benefits of many location services in the future. Ultimately, self-regulation allows the market to choose acceptable business practices without burdensome interference from government regulators.

2. *Wireless Spam: The Coexistence of Self-Regulation and Legislative Proposals*

If the consumer has not consented to receive "push" advertising in the wireless environment, then "spam" becomes a problem when cell phones and pagers ring or beep incessantly with time-sensitive coupons and other location-based offers.[175] The term "spam" is used in the electronic marketplace to describe unsolicited commercial email or junk email. The opportunity to push location-based advertisements to wireless subscribers adds fuel to what privacy advocates and some members of Congress recognize as an impending "air-spam" problem.[176] Some early players in the location services industry have expressed their intention to avoid making PDAs a "spam-happy advertising medium" by using an opt-in model and asking customers to indicate the types of advertisements they might want to receive on their wireless device.[177] Others, however, may have business models that aim to give mobile service providers the opportunity to deliver location-based advertisements to unsuspecting customers using wireless surveillance.[178]

Wireless spam, in the form of a short text message instantly appearing on a PDA screen, may be more intrusive than email spam because consumers will not be able to delete the message without first looking at it.[179] Beyond frustrating consumers, wireless spam will likely affect the technological resources of wireless systems and impact the costs of wireless service.[180] Anticipating continued advances in technology that make it easier to

---

172 FEDERAL TRADE COMMISSION, *In Re* ReverseAuction.com, Statement of Commissioner Mozelle W. Thompson *at* http://www.ftc.gov/os/2000/01/reversemt.htm (Jan. 6, 2000) [hereinafter Thompson Statement] ("[I]f industry 'self-regulation' is to have meaning and if we seek to create an overall market climate in support of data privacy, industry needs to be encouraged to take direct independent action against those who violate the terms of their privacy agreements.").

173 In the online marketplace, businesses that participate in a seal program promise to abide by certain principles or rules propagated by the program's developer. Seal programs developed by TrustE, BBBOnline and WebTrust, for example, are an effort to promote industry self-regulation and consumer privacy protection. Major R. Ken Pippin, *Consumer Privacy on the Internet: It's "Surfer Beware,"* 47 A.F. L. REV. 125, 132 (1999). *See generally* Kalinda Basho, *The Licensing of Our Personal Information: Is It a Solution to Internet Privacy?*, 88 CAL. L. REV. 1507 (2000); Jonathan P. Cody, *Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation?*, 48 CATH. U. L. REV. 1183 (1999).

174 Raul, *supra* note 35; Daley, *supra* note 157 (noting that profiling can benefit both companies and consumers by targeting the right products to the right customers); Alexis D. Gutzman, *Location-based Services for PDAs*, ECOMMERCE-GUIDE.COM, *at* http://ecommerce.internet.com/news/insights/ectech/article/0,,10378_701561,00.html (Feb. 28, 2001) ("M-commerce is about relevancy and immediacy."); *see U.S. West v. FCC*, 182 F.3d at 1235 ("Although we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information may usually pass freely.").

175 Hawkins, *supra* note 30, at 74 ("If customers are overwhelmed by 'air spam' and come-ons, they may boycott wireless applications.").

176 Wireless Telephone Spam Protection Act, H.R. 113, 107th Cong. § 2 (2001)

177 Konrad, *supra* note 145.

178 Hawkins, *supra* note 30, at 74.

179 David Neal, *Newest Bull's-Eye in Spam Wars: SMS*, ZDNET NEWS, *at* http://www.zdnet.com/zdnn/stories/news/0,4586,2693045,00.html (Mar. 6, 2001). In addition, email and Internet viruses may send data to a Short Messaging Service (SMS) gateway that converts email text into telephone signals and then spams random cell phones with the infected message. Brendan I. Koerner, *A Telephone Spam Scam*, U.S. NEWS ONLINE, *at* http://www.usnews.com/usnews/issue/000619/virus.htm (June 19, 2000) (describing how the notorious ILOVEYOU email virus burrowed its way into cell phones in Spain).

180 *See* Jeffrey L. Kosiba, *Legal Relief from Spam-Induced Internet Indigestion*, 25 DAYTON L. REV. 187, 193 (1999) [hereinafter Kosiba] ("[S]ince many e-mail subscribers pay for Internet access on a per minute or per hour basis, using those paid minutes to access, review, and return or discard unsolicited mail that was deposited into their e-mail accounts is, in essence, paying for spam."); Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. 436, 438 (E.D. Pa. 1996) (stating that plaintiff's sending millions of unsolicited emails each day through defendant's servers resulted in overload of the system).

transmit text messages, graphics and images to wireless telephones, Congress is considering the Wireless Telephone Spam Protection Act of 2001 (H.R. 113) in order to protect the privacy of wireless subscribers by prohibiting the transmission of unsolicited commercial messages.[181]

While wireless spam is a new concept, the practice of sending junk mail is not new. "Junk mail, junk faxes, and even telemarketing calls are all unsolicited means by which advertisers promote their products."[182] Offline "spamming" — and profiling — have occurred for years, yet privacy advocates spoke louder when these activities appeared in the electronic marketplace.[183] H.R. 113 represents the latest example of finding new fear in an old practice. Although grounded in firm privacy principles, H.R. 113 does nothing that competent self-regulation and enforcement cannot also do. If enacted, H.R.113 will be open to First Amendment challenges as companies argue for their right to communicate with customers.[184] Such legal challenges could ultimately nullify the proposed law. Therefore, the location services industry must have self-regulatory principles in place as a fallback measure in order to maintain consumer confidence.[185]

Self-regulatory initiatives to combat wireless spam should begin with the requirement of consumer opt-in consent to a service provider's privacy notice for sending location-based short text messages or other advertisements. In Europe, three of Britain's mobile phone companies have taken self-regulatory measures to limit spam delivered to wireless phones.[186] The newly formed Wireless Marketing Association has developed a code of conduct that requires companies to receive a customer's opt-in consent prior to delivering wireless marketing services.[187] In the United States, the Wireless Advertising Association ("WAA") has offered a set of anti-spam principles for its members, declaring (among other things) that members should not send wireless push advertising or content without confirmed opt-in customer approval.[188] As additional precautions, WAA principles also prohibit the unauthorized transfer of subscriber data to third parties and condemn forging the identity of message originators, sending chain letters, making "fake" voice calls, and misleading subscribers about content.[189] These issues are not fully addressed by H.R. 113, which may indicate that the industry is better positioned than legislators to develop privacy rules for commercial location service providers.

IV. CONCLUSION

The Wireless Communications and Public Safety Act of 1999 and the FCC's E911 requirements ushered in a variety of new wireless services that use location-tracking technology.[190] As carriers restructure their networks to deploy wireless E911 service by October 2001,[191] third party application providers and content developers are plan-

---

181 H.R. 113.

182 Kosiba, *supra* note 180, at 192.

183 David Freedman, *A Letter to Washington*, eCOMPANY Now, Jan. 2001 *available at* http://www.ecompany.com/articles/mag/print/0,1643,9009,00.html ("Off-line businesses have long relied on this sort of information without creating significant harm, and beyond the naive argument that the Internet should hew to the quasi-utopian standards of its early noncommercial denizens, there is no good reason for the bar to be set far higher online."); *see* Thompson Statement, *supra* note 172 ("[T]he Commission does not here declare that sending unsolicited commercial e-mail ('spamming') is unfair in all circumstances, nor does it suggest that privacy invasions cause substantial injury in all circumstances.").

184 *See Cyber*, 948 F. Supp. 436. In *Cyber*, the plaintiff sued defendant AOL alleging that AOL's attempt to block Cyber's sending millions of unsolicited commercial email on a daily basis through AOL's servers infringed its First Amendment rights. The court found that:

> since AOL is not a state actor and there has been no state action by AOL's activities under any of the three tests for state action enunciated by our Court of Appeals in [*Mark v. Borough of Hatboro*, 51 F.3d 1137 (3rd Cir. 1995)], Cyber has no right under the First Amendment to the United States Constitution to send unsolicited e-mail to AOL's members.

Id. at 445.

See generally Joshua A. Marcus, *Commercial Speech on the Internet: Spam and the First Amendment*, 16 CARDOZO ARTS & ENT. L.J. 245 (1998); Credence E. Fogo, *The Postman Always Rings 4,000 Times: New Approaches to Curb Spam*, 18 J. MARSHALL J. COMPUTER & INFO. L. 915 (2000).

185 Neal, *supra* note 179 (noting that services providers have an interest in maintaining relationships with customers).

186 *Id.*

187 *Id.*

188 WIRELESS ADVERTISING ASSOCIATION, WAA GUIDELINES, PRIVACY AND SPAM, PHASE I *at* http://www.ftc.gov/bcp/workshops/wireless/presentations/depriest.pps (Dec. 11, 2000) (presenting to the Federal Trade Commission Workshop, The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues).

189 *Id.*

190 *See* Sovocool, *FCC Sets the Table*, *supra* note 6; Kupfer, *supra* note 6.

191 47 C.F.R. § 20.18(e).

ning news, navigational, retail and directory services that use the same technology to target customers using wireless devices.[192] The 1999 Act not only served as a catalyst for location-based services, it also obligated carriers to protect the confidentiality of customers' location information generated in the provisioning of service.[193]

Under Section 222 of the 1934 Act, wireless carriers are prohibited from using location information for non-emergency purposes or disclosing location information to third parties without the customer's express prior authorization.[194] No such rule governs non-carrier third parties that do not fall under the FCC's jurisdiction over telecommunications service providers.[195] Nonetheless, application and content developers will share responsibility for customer location data when a carrier obtains the customer's consent to release such information to those third parties.[196]

Because legislation governing location services is scarce, both carrier and non-carrier members of the industry have the opportunity to become a model of effective self-regulation for privacy practices in the electronic marketplace. The FTC's Notice, Choice, Access and Security principles, as applied to the location services industry, will help achieve this goal.[197] Providers should make comprehensive privacy policies disclosing their location data gathering, storing and sharing activities available to customers. In turn, customers should have the ability to "opt-in" to location services by providing their express prior authorization. Those customers that have volunteered personal information should have the ability to view, correct or delete information the service provider has collected about them. Finally, service providers should not only take reasonable measures to secure location data from unauthorized access, but they should also address security issues that are unique to the wireless environment, including interception and surveillance. If location service providers take these measures to ensure the confidentiality of location information, then "[e]ach customer will be in control of his or her own privacy, and will be able to choose precisely how much information to forfeit in return for a service."[198]

---

192 *See* Emling, *supra* note 1; Perera, *supra* note 4; Bob Brewin, *Coca-Cola Adds Location-Based Mobile Commerce*, COMPUTERWORLD, Dec. 4, 2000 (reporting Coca-Cola's plans to provide the location of the nearest restaurant, convenience store or gas station serving its products to consumers with a device capable of determining the user's location); Konrad, *supra* note 146.

193 47 U.S.C. § 222(a).

194 SEN. REP. NO. 106-138, at 8, 10. *See* note 12.

195 *See* note 114.

196 Both the FCC and FTC have noted that it would be counterproductive to roll out expensive and sophisticated location determination technology if privacy concerns adversely affect consumer acceptance. *CTIA Seeks Uniform Policy on Location Information, Privacy*, MOBILE COMM. REP., Oct. 30, 2000 (quoting current FCC Wireless Bureau Chief Thomas Sugrue as noting the counterproductive effects of privacy concerns on E911 services); *FTC Forum Targets Privacy, Security of Wireless Internet*, TELECOMMS. REPS., Jan. 8, 2001, at 28 (quoting FTC Commission Mozelle Thompson as identifying issues related to GPS technology and handheld devices as raising major privacy concerns); *see Variety of Wireless Privacy Issues Cited at FTC Event*, COMM. DAILY, Dec. 13, 2000 ("It will be difficult to 'retrofit' privacy and security onto wireless networks once they're completed, so even start-up companies need to think about those issues now.").

197 *See* FTC REPORT TO CONGRESS, *supra* note 92, at iii.

198 Raul, *supra* note 35.