Private Eyes Are Watching You: With the Implementation of the E-911 Mandate, Who Will Watch Every Move You Make?

Geoffrey D. Smith*

I. INTRODUCTION

After a snowmobile accident broke his neck, back, ribs, and bruised his lung, Brent Alvut managed to dial 911 from his cellular phone.[1] The

*B.S. 1996, Purdue University; J.D. Candidate, Indiana University School of Law–Bloomington. I would like to thank my family and friends for their support and the Editorial Board of the *Federal Communications Law Journal*, for its assistance throughout the writing process.

1. Kathryn Balint, *Cell Phones Can Leave 911 Operators Guessing*, COPLEY NEWS SERV., Nov. 7, 2004.

global positioning system ("GPS") technology integrated within his cellular phone allowed the 911 operator to immediately pinpoint Alvut's location and save his life.[2]

Many were not as fortunate as Brent. In 1993, eighteen year old Jennifer Koon called 911 from her cell phone, however, she was unable to tell the dispatcher her location.[3] The dispatcher "listened helplessly . . . as Koon was raped and killed."[4] In 2001, a thirty-two year-old woman drove off of the Florida Turnpike, into a canal.[5] As her car was sinking, she dialed 911.[6] She talked to the dispatcher for over three minutes but did not know her exact location.[7] Rescuers were unable to find her before she died.[8]

Stories abound of men, women, and children who were stranded in places unknown; who were trapped under the September 11th rubble; who were abducted; who were lost in the snow; and others who were carried away by the tsunami in Southeast Asia. All found themselves in a place they could not describe, and many could have been saved had their location been immediately known.

In the United States, there are nearly 200,000 911 calls made by cell phones every day.[9] In response, the Federal Communications Commission ("FCC") has developed a set of regulations called Enhanced 911 ("E-911") that require wireless carriers to identify the location of the caller's cellular phone for the delivery of emergency services.[10] Once E-911 is fully implemented, emergency operators will automatically receive the callers' location without wasting valuable time seeking information from a caller who may not be able to sufficiently describe their location.[11] By December 31, 2005, wireless carriers must ensure that 95% of their subscribers have cellular phones with location-tracking technology.[12] This will complete the

---

2. *Id*.

3. *Id.*

4. *Id.*

5. Steven Isbitts, *Counties Quiet About 911 Cell Phone Tracking*, TAMPA TRIB., Oct. 2, 2003.

6. *Id.*

7. *Id.*

8. *Id.*

9. Balint, *supra* note 1.

10. FTC, PUBLIC WORKSHOP: THE MOBILE WIRELESS WEB, DATA SERVICES AND BEYOND: EMERGING TECHNOLOGIES AND CONSUMER ISSUES 9 (2002) [hereinafter PUBLIC WORKSHOP].

11. *Id.*

12. Request by Cellular Telecommunications and Internet Association to Commence Rulemaking to Establish Fair Location Information Practices, *Order*, 17 F.C.C.R. 14382, para. 7 (2002) [hereinafter *CTIA Request*].

four-year rollout of the FCC's wireless E-911 program.

The E-911 program will undoubtedly save lives, and wireless carriers are using cell phone location information for alternative services.[13] Location Based Services ("LBS") have already and will continue to add many benefits to our lives. Some employers already use the technology to keep track of their employees, and some parents use it to keep an eye on their children.[14]

Despite the many benefits, privacy advocates have expressed concern over the potential to collect, store, and analyze every place individuals go with their cell phone.[15] Are wireless carriers permitted to track, record, and store every location your cell phone travels? Can third-party service providers record, store, and sell your location information? Has the government effectively gained access to most individuals' daily routines, the places they visit and even whom they visit?[16]In an attempt to address privacy concerns with E-911, Congress requires that wireless carriers obtain "express prior authorization" before releasing location information to third parties.[17] Industry advocates requested the creation of regulations to clarify the meaning of "express authorization" and "location information"; however, the FCC declined the request, stating that the statutory language was clear.[18]

Are additional limitations on the collection, storage, and use of personal location information needed? To address this question, this Note will consider the history of the Wireless Communication and Public Safety Act of 1999 and the potential problems with the current statutory

---

13. Aaron Renenger, *Satellite Tracking and the Right to Privacy*, 53 HASTINGS L.J. 549, 552–53 (2002).

14. David Colker, *Big Brother Really is Watching with GPS*, L.A. TIMES, Jan. 7, 2005; George Brandon, *New Cell Phones Let Firms Track Workers*, KIPLINGER BUS. FORECASTS, Dec. 29, 2004.

15. PUBLIC WORKSHOP, *supra* note 10, at 8.

16. The government is relevant to the concerns of private company access. While the fourth amendment provides some protection from government intrusion into private affairs, this is less so after *U.S. v. Miller*. In U.S. v. Miller, 425 U.S. 435 (1976), the Supreme Court held that financial records controlled by a third party were not protected by the Fourth Amendment. Id. at 443. Therefore, the government was able to collect indirectly what it would not constitutionally be allowed to collect directly. The Court stated that since the individual voluntarily gave the information to the third party, the government could obtain that information from the third party. Therefore, the same principle would likely apply here, if the wireless carrier is able to store the movements of your cell phone, now the government can obtain that information from your wireless carrier with a record of, inter alia, all your movements and daily habits.

17. *Id.* at 10; CTIA Petition for Rulemaking to Establish Fair Location Information Practices, *Reply Comments of Electronic Privacy Information Center*, at 8 (2001), http://www.epic.org/privacy/wireless/epic_reply.pdf.

18. *CTIA Request*, *supra* note 12, para. 1.

protection. This Note will argue that the current statutory provisions along with the Federal Trade Commission's ("FTC") unfair and deceptive act are inadequate to protect against the potential for abuse of personal location information. Self-regulation has failed with the Internet and is unlikely to succeed in the wireless environment.[19] Therefore, additions to Section 222 of the Telecommunications Act of 1996 ("1996 Act") are needed to ensure protection of individual location information. By making limited additions, individuals can enjoy both the benefits of increased privacy protection without hindering the industry's development of LBS.

II. PRIVACY LAW ORIGINS AND THE POTENTIAL FOR HARM IN THE COLLECTION OF PERSONAL LOCATION INFORMATION

Privacy law in the United States began with the publication of *The Right to Privacy* in the *Harvard Law Review*.[20] Louis Brandeis and Samuel Warren expressed concern that the instant photograph would allow the press to overstep "in every direction the obvious bounds of propriety and of decency."[21] Brandeis and Warren defined privacy as "the right to be let alone" and established the "foundation for the two dominant strands of U.S. privacy law: protection against government invasions of citizen privacy, and protection against harmful uses of personal information."[22]

The protection against harmful uses of personal information is found in the development of three common law torts: (1) the tort of unreasonable intrusion into the seclusion of another, (2) the tort of unreasonable publicity given to the other's private life, and (3) the tort of publicity that unreasonably places the other in a false light before the public.[23] These torts were designed to apply only to "a narrow category of harmful uses of information."[24] The torts must also withstand First Amendment review. Since the courts have long held that there is no expectation of privacy in a public place, it is unlikely that any of these torts would be applicable to personal location information collected in the public.[25]

---

19. Ellen Traupman, *Who Knows Where You Are? Privacy and Wireless Services,* 10 COMMLAW CONSPECTUS 133, 152 (2001).

20. Fred H. Cate, *The Privacy Problem: A Broader View of Information Privacy and the Costs and Consequences of Protecting It*, 4 FIRST REP. 1, 3 (Mar. 2003), *available at* http://www.freedomforum.org/templates/document.asp?documentID=17631.

21. *Id.*

22. *Id.*

23. *Id.* at 4.

24. *Id.* The privacy torts only apply when the information is "highly offensive to a reasonable person" and either false or of no "legitimate public concern." *Id.*

25. Cate*, supra* note 20, at 4–5.; James C. White, People, Not Places: A Policy Framework for Analyzing Location Privacy Issues 1 (Spring 2003) (unpublished M.A. Thesis, Duke University), http://www.epic.org/privacy/location/jwhitelocationprivacy.pdf;

The other strand of U.S. privacy law, protection against government invasion of citizen privacy, has developed through the Supreme Court's interpretation of the Constitution.[26] Although the Constitution provides no explicit right to privacy, the Supreme Court has found a right to privacy in the "shadows" of the Bill of Rights.[27] This right protects individuals from the government's invasion of privacy, but does not provide protection between individuals and businesses.[28]

This focus on government intrusion reflects the reality that only the government exercises the power to compel disclosure of information and to impose civil and criminal penalties for noncompliance. Only the government collects and uses information free from market competition and consumer preferences. "It is therefore not surprising that the Supreme Court has interpreted the Bill of Rights to restrict the government's collection and use of personal information."[29]

Today, this brightline distinction between the government and the private sector may not be warranted.[30] New technologies allow the private sector to collect and store tremendous amounts of personal information.[31] Once the information is collected in the private sector, the government is not prohibited from accessing the information.[32]

These technological developments show good cause for consumer concern. The government has issued the E-911 mandate requiring wireless carriers to implement technology with the capability of collecting and storing personal location information.[33] The government has not put restrictions on the collection and storage of the personal location information that may be collected by the wireless carriers. Furthermore, once the wireless carriers and third-party service providers collect the information, the government is then able to access the stored information.[34] Therefore, the government has enabled itself to collect personal location information indirectly, which it most likely would have been prevented from doing under the Constitution. Since most Americans either carry, or

---

Renenger, *supra* note 13, at 558.

26. Cate, *supra* note 20, at 4.

27. White, *supra* note 25, at 7.

28. Cate, *supra* note 20, at 4; Renenger, *supra* note 13, at 555–56; *see also* Fred H. Cate & Robert Litan, *Constitutional Issues in Information Privacy*, 9 MICH. TELECOMM. TECH. L. REV. 35, 40 (2002).

29. Cate, *supra* note 20, at 4.

30. *See* Cate & Litan, *supra* note 28, at 62.

31. *Id.*

32. *Id.*

33. FCC, Enhanced 911—Wireless Services, www.fcc.gov/911/enhanced (last visited Apr. 21, 2006).

34. *See* Cate & Litan, *supra* note 28, at 62.

will eventually carry, a cell phone with them everywhere they go, the government is effectively able to track all of the movements of an individual's cell phone, gaining access to the places and people the individual visits.

In addition to concern over governmental access to such personalized information, other harms or concerns have been raised. Some consider it a harm that every place to which an individual travels may be recorded, analyzed, and stored indefinitely. Furthermore, this may influence the individuals' freedom of action and may even impede political dissent. If the individuals are not aware that the data is being collected, they may be harmed if the data contains errors or is misattributed to them. To some, the collection of personal location information may be embarrassing or may be seen as a violation of each individual's autonomy.

Often the disclosure of the information is not the harm itself, but rather the intervening factor that leads to a harm. For instance, information that is disclosed to a stalker harms the individual due to the actions of the stalker. Disclosure to a marketer may result in the harm of the nuisance of unwanted sales solicitations. With today's national security concerns, the greatest threat may be a terrorist who accesses location information to maximize casualties.

Despite the common difficulty in articulating a specific harm, "the dominant trend in recent and pending privacy legislation is to invest consumers with control over information in the marketplace, irrespective of whether the information is, or could be, used to cause harm."[35] Since the individual lacks both constitutional and common law protection, any control over personal location information must come through statutory law.

III. LEGAL HISTORY OF FEDERAL REGULATION FOR CELL PHONE LOCATION INFORMATION

A. Telecommunications Act of 1996 and U.S. West v. FCC

In 1996, Congress passed Section 222 of the 1996 Act requiring customer approval before distributing customer proprietary network information ("CPNI") to third parties.[36] In 1998, the FCC created an opt-in

35. Cate, *supra* note 20, at 5.

36. U.S. West, Inc. v. FCC, 182 F.3d 1224, 1229 (10th Cir. 1999); Waseem Karim, Note, *The Privacy Implications of Personal Locators: Why You Should Think Twice Before Voluntarily Availing Yourself to GPS Monitoring*, 14 Wash. U. J.L. & Pol'y 485, 498 (2004). Customer proprietary network information is defined as:

> (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service

regulation to clarify the way in which companies could obtain customer approval.[37] The regulation required the wireless carrier to obtain "prior express approval from a customer through written, oral, or electronic means before using the customer's CPNI."[38]

One year later, U.S. West challenged the FCC's opt-in regulation as an undue restriction on commercial speech under the First Amendment.[39] Furthermore, U.S. West argued that the regulation raised Fifth Amendment concerns as the CPNI was valuable property belonging to U.S. West.[40] The Tenth Circuit Court of Appeals determined that the regulation was "presumptively unconstitutional unless the FCC could prove otherwise by demonstrating that the rules were necessary to prevent a 'specific and significant harm' to individuals, and that the rules were 'no more extensive than necessary to serve [the stated] interests.'"[41] The FCC subsequently adopted the less restrictive opt-out standard, requiring customers to contact the wireless carrier to prevent their personal information from being distributed to third parties.[42]

B. Wireless Communication and Public Safety Act of 1999

The 1999 Wireless Communications and Public Safety Act ("WCPSA") amended Section 222 of the 1996 Act.[43] The definition of CPNI in Section 222(h) was amended to include "location" as information that carriers must protect.[44] Congress also added Section 222(f) which "restrict[s] carriers' authority to access, use, or disclose wireless location information 'without the express prior authorization of the customer,'

> 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) (2000).

37. *U.S. West*, 182 F.3d at 1230. An opt-in regulation requires the user to take affirmative steps in order for the business to use the individual's personal information. An opt-out regulation allows the business to use the individual's personal information unless the individual takes affirmative steps to prevent the business from using his or her personal information. Since most people do not take affirmative action either way, the default setting determines the category that the majority of consumers fall under. *See* Traupman, *supra* note 18, at 139.

38. *U.S. West*, 182 F.3d at 1230.

39. *Id.*

40. *Id.*

41. Cate, *supra* note 20, at 12 (quoting *U.S. West*, 182 F.3d at 1235).

42. David J. Phillips, *Beyond Privacy: Confronting Locational Surveillance in Wireless Communication*, 8 COMM. L. & POL'Y 1, 13–14 (2003).

43. *CTIA Request*, *supra* note 12, para. 2.

44. *Id.*; 47 U.S.C. § 222(h).

except in three specifically established emergency situations."[45]

In 2000, the Cellular Telecommunications and Internet Association ("CTIA") petitioned the FCC to create regulations clarifying the Section 222 amendments.[46] CTIA expressed concern over how "express prior authorization" would be defined and argued that the lack of clarity would slow the adoption of location enabled services.[47] The CTIA petition sought to ensure that wireless consumers are (1) informed of location information collection (notice), (2) given the opportunity to consent to collection of the location information (choice), and (3) assured the location information is secure and accurate (access and security).[48] Further criticism was aimed at the limited protection in the amendment against redisclosure of location information by third parties who have access to location information through the wireless provider.[49]

Despite the concerns voiced by privacy advocates, in 2002, the FCC formally declined to adopt regulations for the Section 222 amendments.[50] The FCC concluded that the statutory language was not ambiguous "Because the statute imposes clear legal obligations and protections for consumers and because we do not wish to artificially constrain the still-developing market for location-based services, we determine that the better course is to vigorously enforce the law as written."[51]

The order stated that Section 222(f)'s requirement of "express prior authorization" clearly indicates that consumers must give "explicitly articulate approval"[52] (opt-in) before their location information may be used. Therefore no regulations were necessary.[53]

In addition to amending Section 222, the WCPSA also enabled the FCC's E-911.[54] The first phase required wireless carriers to report to a Public Service Answering Point ("PSAP") the telephone number of a

45. *CTIA Request*, *supra* note 12, para. 2 (quoting 47 U.S.C. § 222(f)). The three emergency situations where disclosure of personal location information is allowed include: (1) disclosure to an emergency medical service provider, fire service, or law enforcement in response to a call for emergency services; (2) to inform a legal guardian or parent of the location of a child in an emergency involving the death or serious harm to the child; (3) disclosure to database management services "solely for purposes of assisting in delivery of emergency services in response to an emergency." 47 U.S.C. § 222(d)(4)(C).

46. *See CTIA Request*, *supra* note 12, para. 3.

47. *See CTIA Request*, *supra* note 12 (statement of Michael J. Copps, Comm'r, dissenting).

48. *See id.*

49. PUBLIC WORKSHOP, *supra* note 10, at 11.

50. *See CTIA Request*, *supra* note 12, para. 1.

51. *Id.*

52. *CTIA Request*, *supra* note 12, para. 5.

53. *Id.*

54. White, *supra* note 25, at 22.

wireless 911 caller and the location of the cell tower through which the call was made.[55] The second phase of the E-911 program, which was to be completed by December 31, 2005, requires wireless carriers to locate a cellular phone within 50 to 300 meters of its true location.[56] This initiative requires wireless carriers, public safety agencies, and equipment manufacturers to upgrade their facilities, and the implementation is expected to cost several billion dollars throughout the wireless service industry.[57]

With so much money invested in E-911, it is not surprising that wireless carriers are finding ways to put the service to commercial use.[58] Location-based services are being developed that provide customers with information to traffic, weather, and retail stores based upon their geographical position at any given time.[59] Google has created a test service that allows consumers to search from their mobile phones to find the nearest business and even allows customers to compare prices against the prices of online stores.[60] Others are developing services that allow the consumer to check gas prices at nearby stations so that the consumer can easily go to the station with the lowest price.[61]

Also, businesses have begun using location tracking in cellular phones to keep tabs on their employees and increase productivity.[62] For example, companies have begun monitoring their mobile workforce using cell phones with location tracking technology.[63] The technology allows businesses to monitor their employees, to dispatch them for rush jobs, and even to provide assistance in finding a new customer location.[64]

Likewise, parents are using the technology to keep an eye on their children.[65] Some services will alert the parent if the child leaves a

---

55. FCC, Enhanced 911—Wireless Services, http://www.fcc.gov/911/enhanced/ (last visited Apr. 22, 2006).

56. *Id.*

57. *Id.*; Aaron Futch & Christine Soares, *Enhanced 911 Technology and Privacy Concerns: How has the Balance Changed Since September 11?*, 2001 DUKE L. & TECH. REV. 0038, para. 4 (2001).

58. PUBLIC WORKSHOP, *supra* note 10, at 10.

59. *Id.* at 4.

60. Google, Google Short Message Service, http://www.google.com/sms (providing a service that allows text messages for local business listings, driving directions, movie showtimes, weather updates, and product prices) (last visited Apr. 22, 2006).

61. Finding cheap gas via cell phone, WNDU NEWS CENTER 16, Sept. 27, 2004, http://www.wndu.com/news/contact16/092004/contact16_37574.php.

62. Brandon, *supra* note 14.

63. *Id.*

64. *Id.*

65. Colker, *supra* note 14.

designated area or begins traveling over a designated speed.[66] Additionally, others have used similar services to prevent frantic searches for Alzheimer's patients, and one woman used the technology to catch her husband in a lie: her husband claimed to be working late when he was actually going to the Holiday Inn.[67]

Potential abuses of the technology are not hard to imagine. With many people now carrying a cell phone everywhere they go, wireless carriers can now collect tremendous amounts of information about an individual. Databases could store information regarding every place you have been and, through data processing, can even determine the people you were traveling with at that time.

Uncomfortable uses of the technology have already been suggested. For example, imagine an employer who refuses to hire someone after determining that the candidate routinely visits an AIDS clinic or an insurance company that charges higher rates for those taking part in dangerous activities (e.g., rock climbing, sky diving, or late night bar hopping).[68] Imagine a business that purchases the location information of the salesmen of its primary competitor, instantly gaining access to every company with which the competitor does business.[69] Once location information is distributed to other parties and combined with other personal information, it is hard to imagine any information—other than personal thoughts—remaining private.

Despite the rapid development of commercial uses for location services, there are two important questions that remain unanswered. First, will the opt-in requirement of the Section 222 amendments withstand a commercial speech challenge? Although important, this question is beyond the scope of this Note, but other articles have addressed it.[70] Second, what type of action may a consumer take if a wireless carrier violates the 1996 Act?[71] Imagine a consumer's surprise after agreeing to opt-out of location tracking, only to later learn that his location history has been collected and distributed to third parties and that the consumer has no significant recourse.[72]

---

66. *Id*. The child was traveling over the speed limit heading out of state as the parent watched from the computer at home. The parent called the child and told him to slow down.

67. *Id.*

68. *E.g.*, Renenger, *supra* note 13, at 553, 557.

69. Kristen E. Edmundson, Note, *Global Positioning System Implants: Must Consumer Privacy Be Lost in Order For People To Be Found?*, 38 IND. L. REV. 207, 215 (2005).

70. Renenger, *supra* note 13, at 561.

71. *Id.* at 561–62.

72. *See id*.; *see also* White, *supra* note 25, at 25 (discussing *Conboy v. AT&T*). Despite obvious violations of the Communications Act, *Conboy v. AT&T* was dismissed on summary judgment because actual damages could not be shown. Since the unauthorized

C. Federal Trade Commission's Unfair and Deceptive Act

Other areas of federal law also provide little protection for the individual. The FTC uses both it's unfairness doctrine and it's deceptive practices doctrine to prevent injuries to consumers.[73] Recently, the FTC has used the unfairness doctrine to bring charges against businesses that failed to adequately protect sensitive consumer information.[74] However, since location information is included within the definition of CPNI under the Communications Act, the protection of location information by wireless carriers is likely outside the jurisdiction of the FTC's unfairness doctrine.[75]

Even though the unfairness doctrine is unlikely to apply, the deceptive doctrine should apply to third party service providers and possibly to the wireless carriers. Once the E-911 mandate is implemented, location information is likely to be stored and analyzed by wireless carriers and third parties.[76] The exchange and use of this information may be governed by the carrier's privacy policy and customer agreements, and thereby regulated by the FTC.[77] The FTC has ruled that a violation of the company's privacy statement is an unfair and deceptive practice.[78] Using

---

disclosure of location information may not cause a demonstratable financial harm, the consumer whose information was disclosed is unlikely to survive summary judgment. White, *supra* note 25, at 25.

73. J. HOWARD BEALES, III, BUREAU OF CONSUMER PROTECTION, FTC, THE FTC'S USE OF UNFAIRNESS AUTHORITY: ITS RISE, FALL AND RESURRECTION, http://www.ftc.gov/speeches/beales/unfair0603.htm#N_1_ (last visited Apr. 18, 2006).

74. In June of 2005, BJ's Wholesale Club settled charges brought by the FTC. The FTC alleged that the wholesale club failed to take appropriate security measures to protect consumer's credit and debit card information. This personal information was used to make fraudulent purchases totaling millions of dollars. See Press Release, FTC, BJ's Wholesale Club Settles FTC Charges (June 6, 2005), *available at* http://ftc.gov/opa/2005/06/bjswholesale.htm. More recently, in January of 2006, the FTC settled charges against Choicepoint, which included an alleged violation of both the unfairness doctrine and deceptive practices by making promises that it only provided personal information to those who met ChoicePoint's rigorous credentialing process. Choicepoint provided over 160,000 credit reports to an unauthorized subscriber, which resulted in over 800 cases of identity theft. See Press Release, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006), *available at* http://www.ftc.gov/opa/2006/01/choicepoint.htm.

75. *Protecting Consumers' Phone Records: Hearing Before the Subcomm. on Consumer Affairs, Prod. Safety, and Insurance of the S. Comm. on Commerce, Sci., and Transp.*, 109th Cong. 8 n.21 (2006) (prepared statement of Lydia B. Parnes, Director, Bureau of Consumer Protection, FTC), http://www.ftc.gov/os/2006/02/commissiontestimonypretexting060208.pdf. See also 15 U.S.C. § 45(a)(2).

76. Futch & Soares, *supra* note 57, para. 9.

77. FTC, Privacy Initiatives, Enforcing Privacy Promises: Section 5 of the FTC Act, http://www.ftc.gov/privacy/privacyinitiatives/promises.html (last visited Apr. 22, 2006) [hereinafter Privacy Initiatives].

78. Interview with Fred Cate, Professor, Indiana University–Bloomington School of Law, Director, Center for Applied Cybersecurity Research, in Bloomington, Ind. (Feb. 24,

Section 5 of the FTC Act, the FCC has taken action to enforce companies' promises in their privacy statements to secure personal information.[79]

The FTC uses five principles as a basis for analyzing privacy issues. These principles include: notice, choice, access, security, and enforcement .[80] Notice is considered the most important of these principles.[81] Notice requires that a customer is actually aware of the ways in which his personal information may be used.[82] Therefore, notice that is buried in a long service agreement or hidden on a telephone bill would not ensure that the consumer was given sufficient notice.[83]

Choice means that consumers can make decisions about their personal information that is collected and must agree to use of that data by third parties.[84] Choice may be difficult in the wireless world since consumers will not likely know all the parties that are receiving personal information.[85] Additionally, privacy disclosures are often not easy to understand, and if they are only provided at the establishment of the service, informed consent may be questioned.[86]

Access requires that the consumer has the opportunity to view and challenge the accuracy of the data collected.[87] This provides accountability in the data collection process.[88] One concern here is that it is often expensive for a company to provide access and authenticate consumers' requests to view their collected location information.[89]

Security refers to the protection of the data against unauthorized access.[90] Although the public generally believes that wireless communication is vulnerable to interception over the airwaves, the greater

---

2005).

79. Privacy Initiatives, *supra* note 77.

80. White, *supra* note 25, at 29. Notice the similarities to the CTIA petition, which address the first four principles in its petition, to the FCC. *CTIA Request*, *supra* note 12 (statement of Michael J. Copps, Comm'r, dissenting).

81. White, *supra* note 25, at 29.

82. *Id.*

83. PUBLIC WORKSHOP, *supra* note 10, at 23.

84. White, *supra* note 25, at 29–30.

85. PUBLIC WORKSHOP, *supra* note 10, at 16. The wireless carrier must receive the location information, and often third-party service providers must have the location information in order to provide the location-based service that the customer has requested.

86. *Id.*

87. White, *supra* note 25, at 30.

88. *Id.*

89. FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 17–18 (2000), http://www.ftc.gov/reports/privacy2000/privacy2000.pdf [hereinafter PRIVACY ONLINE].

90. White, *supra* note 25, at 30.

vulnerability is within the carrier network.[91] The wireless community continues to develop technologies that increase both the protection of the consumer's personal information and the consumer's control over the security of that information.[92]

A related security concern is what is sometimes called the "pot of honey" issue. When valuable information is collected and stored, it becomes an attractive target of hackers.[93] One need only to look to the recent breaches of security of the information storehouses of LexisNexis and ChoicePoint to see that personal information has value and is vulnerable to attack.[94]

Enforcement is the type of regulation governing the violation of the four above principles.[95] This can be self-regulation, government regulation, or even civil and criminal lawsuits.[96] Although the FTC has brought a number of cases against Web sites for failure to enforce their own privacy statements, enforcement has generally been limited to payment of the money made from the illegal activity and renewed enforcement of the privacy agreement.[97]

The FTC privacy principles, although seen in varying forms, are consistently used in privacy regulations. The FTC has used these principles and its authority under Section 5 of the FTC Act to bring actions against Web sites that have breached their own privacy agreements. Without further legislation, it is likely that the FTC and industry self-regulation will be a temporary means for regulating the privacy of personal location information.

IV. PROBLEMS WITH CURRENT REGULATION MECHANISMS

The current regulation mechanisms provide minimal protection for location information. Individuals attempting to prevent a wireless carrier from storing their personal location information have little recourse if their requests are ignored. Individuals do have some statutory protection against

---

91. PUBLIC WORKSHOP, *supra* note 10, at 17.

92. *See id.* at 18.

93. Jonathan Krim & Robert O'Harrow, Jr., *Data Under Siege: ID Thieves Breach LexisNexis, Obtain Information on 32,000*, WASH. POST, Mar. 10, 2005, at E1.

94. *Id.*

95. PRIVACY ONLINE, *supra* note 89, at 4–5, 20. The FTC has five principles for analyzing security issues (notice, choice, access, security, and enforcement), the four above are the first four of the five discussed. Enforcement is the fifth principle, which is used to regulate the previous four principles.

96. *Id.* at 4.

97. *See* Gateway Learning Corp, Decision and Order, Dkt. No. C-4120 (Sept. 10, 2004), http://www.ftc.gov/os/caselist/0423047/040917do0423047.pdf.

further dissemination of that information, but the protection is minimal.[98] By considering each of the current regulation mechanisms, it is clear that there is little people can do to ensure the protection of their location information.

As we have already seen, both the Constitution and common law tort law provide little to no protection for individuals against the collection and use of personal location information by private businesses.[99]

Furthermore, the statutory protection is inadequate. Section 222 limits the use of "proprietary information from another carrier for purposes of providing any telecommunications service . . ." but does not clearly limit the use of "proprietary information" by third party service providers.[100] The statute does not limit the collection and storage of location information but only the disclosure of CPNI without consent.[101] Therefore, a wireless carrier that collects and stores individual location information without disclosing it to third parties would not be in violation of the statute.[102]

If a wireless carrier or a third-party service provider disclosed an individual's location information, the individual has no remedy unless the individual can show actual damages. Therefore, the individual must rely on the FCC to take action to fine or penalize the wireless carrier.[103]

Therefore, as the law now stands, protection of location information must be found in a combination of industry self-regulation and FTC enforcement of the wireless carriers' voluntary privacy statements. Self-regulation is based upon the premise that the industry is motivated to protect the privacy of the consumer out of fear of bad publicity or the possibility of a backlash from consumers that are unsatisfied with the privacy protection provided.[104] Advocates of self-regulation often tout the heavy costs and inflexibility of regulatory controls, claiming that they will hinder technological growth and market developments since much of the fundamentals of location services are largely unknown.[105]

However, problems with self-regulation have become apparent with the Internet.[106] Initially, the FTC sought self-regulation of Web sites,

98. *See U.S. West*, 182 F.3d at 1230. The statutory protection requires "express prior authorization," ie: "opt-in" consent, however, with the holding in *U.S. West*, this may be unconstitutional, so one is left with the "opt-out" standard.

99. Cate, *supra* note 20, at 3, 4.

100. 47 U.S.C. § 222(b).

101. *See generally* 47 U.S.C. § 222.

102. PUBLIC WORKSHOP, *supra* note 10, at 10.

103. Conboy v. AT&T Corp., 241 F.3d 242, 250–51 (2d. Cir. 2001).

104. Traupman, *supra* note 19, at 152.

105. *Id.*

106. *Id.*

relying on industry organizations to adopt enforcement mechanisms for violations of the privacy agreements.[107] When most Web sites failed to implement privacy protection for consumers, the FTC reversed itself and asked Congress for legislation to provide consumer protection.[108]

An example that illustrates the failure of self-regulation on the Internet is evident in the sale of personal information by Gateway Learning Corporation. Despite explicit promises in its privacy statement, Gateway Learning rented personal information to marketers.[109] After collecting personal information from customers, Gateway Learning changed its privacy statement, allowing disclosure of the personal information to third parties without the consumer's consent or notification.[110] The FTC and Gateway Learning settled the lawsuit.[111] Gateway Learning gave up the money that it earned from the sale of the personal information and promised not to retroactively sell consumer personal information without consent in the future.[112]

Most scholars have concluded that self-regulation to protect consumer privacy on the Internet has failed.[113] Furthermore, even if the five principles articulated by the FTC were implemented, the principles do not provide adequate consumer protection for location information. First, notice is often buried in a contract or provided in a complicated form at the commencement of service and consumers are often unaware of its existence, providing ineffective notice. Second, choice in this environment is dubious at best. If all the wireless providers require consent to provide location-based services, then there is really no consumer choice at all. The consumer has no bargaining power against the wireless carrier. The consumer is left with the choice of having the cell phone and giving up rights to location information or not having the cell phone and losing the benefits of the E-911 mandate.[114] This effectively defeats the benefit of increased safety through the E-911 mandate.

The FTC's "access" principle is included in the statute; however, it only appears to apply to telecommunications carriers.[115] Access should

---

107. *Id.*

108. *Id.*

109. Press Release, FTC, Gateway Learning Settles FTC Privacy Charges (July 7, 2004), http://www.ftc.gov/opa/2004/07/gateway.htm.

110. *Id.*

111. *Id.*

112. *Id.*

113. Traupman, *supra* note 19, at 152.

114. Furthermore, a consumer that had a cell phone before the E-911 mandate must now give up his or her anonymity to continue to enjoy the other benefits of cell phone use.

115. 47 U.S.C. § 222(c)(2).

apply both to the wireless carrier and all third-party service providers. Therefore, under the FTC privacy principles, access would have to be addressed in the wireless carrier's privacy agreement. Additionally, there is no provision requiring security of the information in the statute, so the security of the information would also fall under the regulation of the privacy policy through the FTC. Since each individual company can determine its own level of security and is only held accountable for breaking promises as stated in the privacy statement, the protection provided by the FTC is inadequate.

Currently the FTC guidelines are also inadequate, in that there is not a sufficient remedy. Enforcement of violations of the Web site's own privacy statements has traditionally required the company to adhere to its stated privacy statement and pay a fine equivalent to the amount the company made by selling the personal information that was promised not to be disclosed.[116] At this point the harm has been done, as the information is now in the marketplace and can be freely distributed.[117] In order to recover damages or penalize the policy violator, the consumer would be required to show a specific injury for the harm suffered due to the illegal disclosure. Since in most cases the harm is annoyance or uneasiness in knowing that very personal information is being processed and made available to others, it is unlikely that the consumer can recover any damages from the wireless carrier or encourage future compliance.

Furthermore, the companies create their own privacy policies. There is no affirmative requirement that a privacy policy be developed. Even if the company does create a privacy policy, there are no requirements as to what must be included. Finally, most people do not read the privacy policy.[118] Therefore a company could create a policy with no privacy protection for the customer.

Despite the failure of self-regulation on the Internet, the wireless industry is at work developing technological solutions to improve the

116. The FTC Web site lists the cases that have been settled. Professor Cate says that all of the actions brought by the FTC under Section 5 of the Act for violations of a Web site's privacy statement have settled. FTC, Enforcement, http://www.ftc.gov/privacy/privacy initiatives/promises_enf.html (last visited Apr. 26, 2006).

117. *See*, *e.g.*, Bartnicki v. Vopper, 532 U.S. 514, 529–30 (2001) (holding that once illegally obtained information is possessed by a law abiding citizen, only in rare cases will the law abiding citizen be prevented from freely sharing the information with the public).

118. For example, an independent research firm found that "in 2002 an average of .3% of Yahoo users read its privacy policy. Even at the height of the publicity firestorm created in March 2002 when Yahoo changed its privacy policy to permit advertising messages by e-mail, telephone and mail, that figure rose only to 1%." Cate, *supra* note 20, at 19 (citing Saul Hansell, *Compressed Data: The Big Yahoo Privacy Storm That Wasn't*, N.Y. TIMES, May 13, 2002, at C4).

privacy and individual control of location information.[119] Ideas such as digital rights management would allow consumers to determine specifically which parties had access to their data.[120] Others are considering the use of a proxy to create privacy preferences for a user and similar solutions that allow changes to the preferences depending upon the time and the circumstances, which allows the creation of "work," "home," and "anonymous" personas to determine what information is transmitted.[121]

Alternatively, a consumer concerned about privacy could purchase a prepaid disposable phone, which would allow the consumer to call anonymously and still have the safety benefits of the E-911 mandate.[122] However, this solution does not allow the consumer the full benefits of using a cell phone for other uses, such as a PDA, or new features such as paying for items from a cell phone.[123]

Qualcomm and Lucent have developed phones that allow the user to turn off the location tracking from the handset.[124] However, it is not clear whether the location is simply not shared with third parties or not available to the wireless carrier. ClickaDeal.com, a company designed to provide location-based coupons, has indicated that its company will purge users' location information every hour so that it does not have a history of consumers' movements.[125]

Although these options are encouraging steps towards the protection of consumers' location information, they are incomplete solutions. First, consumers still lacks a remedy if the product fails. Second, in most circumstances, location information may still be shared and analyzed indefinitely. Therefore, the technological advances are encouraging but insufficient to adequately protect or allow control over location information.

All of the current mechanisms available to protect individuals' location information are insufficient. The Constitution provides no individual protection against private industry, Section 222 of the 1996 Act provides minimal protection, and it is unclear if Section 5 of the FTC Act provides any protection to the individual. As the law now stands, the individual cannot prevent a wireless carrier from collecting and storing

---

119. PUBLIC WORKSHOP, *supra* note 10, at 16.

120. *Id.* at 17.

121. *Id.*

122. Laurie Thomas Lee, *Can Police Track Your Wireless Calls? Call Location Information and Privacy Law*, 21 CARDOZO ARTS & ENT. L.J. 381, 405 (2003).

123. PUBLIC WORKSHOP, *supra* note 10, at 3, 7.

124. Lee, *supra* note 119, at 405; Jon Van, *Privacy a Problem with Locator Phones*, CHI. TRIB., Jan. 24, 2004, at C3.

125. PUBLIC WORKSHOP, *supra* note 10, at 16.

personal location information that may be used at a later date or even shared with the government.

V. NEW AMENDMENTS TO SECTION 222 OF THE 1996 ACT ARE NEEDED

Cell phones are being used for more and more purposes every day. Today's cell phones are used to send text messages, to send and receive e-mail, to access the Internet, to receive Amber Alerts, to track employees and children, and to take pictures and video. Cell phones are used as personal organizers, walkie talkies, and MP3 players. Cell phones will soon be used to purchase items, to check competitor's pricing, and to translate language.[126] With so many uses and the added benefit of the E-911 mandate, it is not hard to imagine that most people will take their cell phone with them wherever they go.

This location-tracking technology that follows the movements of your cell phone can soon create a detailed map of everywhere you have gone, when you went there, and who was with you at the time. This information has value and consumers should control its use.[127]

As the law now stands, consumers will inevitably be faced with the decision to receive enhanced location-based services in exchange for their right to their personal location tracking-information. Since most people do not bother to read the privacy notice, it is unlikely that consumers will object.[128] This is especially true if the provision is included in the initial contract for service. Furthermore, if consumers do object, there is no bargaining power on their behalf. Therefore the consumer is left with a take-it-or-leave-it option.

Legislation is needed to help protect people who cannot protect themselves. Further amendments to Section 222 will allow increased consumer privacy without significantly inhibiting the free flow of information and technological growth. Legislation should prevent wireless carriers and third-party service providers from collecting and storing personal location data beyond what is needed for billing purposes. The goal of the legislation would be to prevent the wireless carrier, third parties, and the government from having a historical database of everywhere individuals go. Once this information is collected and combined with other personal information, virtually all individuals with a cell phone will lose all personal privacy with respect to the places they go and the people they

126. Wikipedia, Mobile Phone, http://en.wikipedia.org/wiki/Cell_phone (last visited Apr. 19, 2006).

127. Cate, *supra* note 20, at 5–6.

128. *Id*. at 18.

visit.

Therefore, Congress should amend Section 222 of the 1996 Act to provide individuals with protection of their personal location information that they cannot achieve on their own. Three additions to the 1996 Act will ensure consumers that their private personal location information can be protected in most circumstances and still allow wireless carriers and third parties to provide additional location-based services.

First, the legislation should add a strict liability element for unauthorized access to personal location information. Adding a phrase to Section 222 such as, the wireless carrier and approved third-party providers "shall take such actions as are necessary to prevent unauthorized access to such [personally identifiable] information by a person other than the subscriber . . . [,]" wireless carrier, or third-party provider.[129] The emergency exceptions in Section 222 should continue to apply. This language allows the service provider to determine the means for preventing unauthorized access, while imposing liability for failure to accomplish the objective. This strict liability for disclosure will be subject to the exceptions presently in Section 222. However, it would provide clear language for enforcement of a violation.

Second, Section 222 should include a "destruction of information" requirement. It should state that the wireless carrier and third-party service providers "shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected."[130] This would prevent the wireless carrier and third-party service providers from collecting and storing information regarding a location a person visits. However, it would still allow for the collection of information for billing purposes and providing location-based services. This addition to the statutory language would also solve the problems of inadequate notice and choice by limiting the collection, storage, and distribution of location information.

Finally, Section 222 should add sections regarding civil action damages, attorney fees costs, and punitive damages. This would allow an individual wronged by an act of a wireless carrier to bring a civil action in federal court. The court should award damages that are higher than actual damages—but set at some minimum level—and should allow punitive damages and reasonable attorney fees. By granting a remedy to the customer, the wireless carrier and third-party service providers will be held

129. 47 U.S.C. § 551(c)(1). This language was taken from the Cable TV Act. The language provides clear and concise requirements and is a similar strict liability, privacy statute.

130. 47 U.S.C. § 551(e).

accountable for violations of the improper collection and disclosure of the personal location information, but will not be inhibited from developing and using LBS.

By implementing these amendments to Section 222, the goals of increased information flow and individual privacy can be effectively reached. Individuals can be assured of the protection of their personal location information and can take the necessary actions for infringement of their privacy. The strict liability language of the statute will allow service providers to compete on a level playing field. Wireless carriers and service providers can freely develop their own services and compliance requirements without limiting statutory requirements, as long as the end result of personal information protection is reached. This allows the providers to determine the best way to protect individuals' location privacy since the company is held accountable for results, specifically that the location information collected to provide the LBS will be destroyed on a timely basis.

VI. CONCLUSION

Privacy means different things to different people.[131] Personal information on consumer habits is very valuable, and it is likely that the wireless industry will seek to extract that value.[132] With cell phones becoming ever more popular, and with the high probability of the cell phone being strongly tied to an individual, the potential for collection of vast amounts of personal data is high.[133] The ability to physically locate an individual who calls 911, saving precious time that will save lives is a great benefit. Many will certainly embrace and use new location-based services for improvement of their lives. However, along with these benefits is the potential for abuse that until now, was not technologically possible. With the ability to locate individuals through their cell phone comes the ability to track that individual virtually everywhere they go. Although technological advances are eroding individual privacy, the potential loss of privacy through cell phone tracking is enormous.

To effectively address this concern, further legislation is needed. Three additions to Section 222 of the 1996 Act will provide individuals with assurance that their location information will be protected. First, by adding a strict liability requirement for unauthorized access to the location information, security of the location information can be enforced. Second, a destruction of information requirement will prevent unlimited collection of

131. Cate, *supra* note 20, at 2.

132. *Id*. at 6.

133. PUBLIC WORKSHOP, *supra* note 10, at 11–12.

location information. Finally, by adding a personal cause of action with punitive damages, the individual can take affirmative action in the event of a violation of the 1996 Act.

Personal privacy is being eroded on all sides. Technological advances have improved our lives in many ways; however, the advances have also increased the means and ways of collecting and storing information on individuals. Since cell phone services are unique in that they have the ability to track your location throughout each day, cell phones pose a unique security and personal privacy risk. In order to ensure that personal privacy is not completely removed, additional legislation for personal location information is needed.