ENHANCED 911 TECHNOLOGY AND PRIVACY CONCERNS:

HOW HAS THE BALANCE CHANGED SINCE SEPTEMBER 11?

E911 technology allows for the location of a cellular phone to be determined by the wireless service provider within several hundred feet. As a consequence, privacy groups have been extremely resistant to the implementation of E911. In the wake of the September 11 tragedies, however, the balance between privacy concerns and national security seems to have changed for many American citizens. This iBrief will explore the nature of the E911 technology, the FCC implementation requirements, the concerns of privacy groups regarding its implementation, and how the environment surrounding E911 has changed since September 11.

Introduction

With over 120 million subscribers in the United States, cellular telephones have rapidly become a fixture in our everyday lives.[1] Cellular phones have also become invaluable in emergency situations; half of all incoming 911 calls are now made from mobile telephones.[2] To enhance the response capabilities of emergency personnel to 911 calls made from cellular telephones, the Federal Communications Commission passed regulations in 1997 that would have required the cellular telephone industry to complete the implementation of Enhanced 911 (E911) technology by October 1, 2001.[3] E911 technology allows for the location of a cellular phone to be determined by the wireless service provider within several hundred feet. As a consequence, privacy groups have been extremely resistant to the implementation of E911 for fear that cellular phones might be turned into tracking devices for the benefit of both the government and private businesses. In the wake of the September 11 tragedies, however, the balance between privacy concerns and national security seems to have changed for many American citizens.

This iBrief will explore the nature of the E911 technology, the FCC implementation requirements and the concerns of privacy groups regarding its implementation. Finally, the iBrief

---

[1] Elizabeth Douglass, Cell Phones Set to Track Call Locales, at http://www.latimes.com/technology/la-000082963oct18.story?coll=la%2Dheadlines%2Dtechnology (last visited October 18, 2001)

[2] *Id.*

[3] *See* Matthew Mickle Werdegar, Note, *Lost? The Government Knows Where You are: Cellular Telephone Call Location Technology and the Expectation of Privacy,* 10 Stan. L. & Pol'y Rev 103, 105 (1998).

will examine whether the changed climate of the country since September 11 has had an impact on the position of the privacy groups and the legislative measures being developed to address E911 privacy issues.

Background

What is E911 Technology?

Enhanced 911 service, also known as E911, permits emergency response personnel to pinpoint the location of a cellular telephone caller anywhere in the United States.[4] While 911 operators are currently able to determine the location of a caller through the use of telephone records when a call is placed from a traditional landline telephone,[5] it is clearly more challenging to pinpoint the location of a cellular phone.

There are two different ways that the location of a cellular phone may be determined. The position may be tracked through the handset itself by using a built-in global positioning system (GPS).[6] Alternatively, the wireless service provider may locate a cellular telephone through triangulation data collected by the network of cellular receiving towers.[7] While local telephone companies have been able to provide landline telephone listing information to 911 services at little additional cost, the implementation of either of the proposed E911 technologies would result in costs of several billion dollars throughout the wireless service industry.[8]

The FCC Requirement for Implementation of E911 Technology

According to the FCC, the implementation of E911 technology is critical to the advancement of public safety.[9] Envisioning this technology as useful for responses to car accidents in remote parts of the country as well as national catastrophes, the FCC first explored the utility of E911 technology in 1996 and issued final regulations in December 1997. The goal of these regulations is to bring wireless 911 service up to the same level as the emergency

---

[4] Elisa Batista, *No Last-Minute Rush for E911, at* http://www.wired.com/news/wireless/0,1382,47220,00.html(last visited Oct. 5, 2001)
[5] Werdegar, *supra* note 2, at 105.
[6] *Id.*
[7] Federal Communications Commission, *FCC Wireless 911 Requirements, at* http://www.fcc.gov/e911/factsheet_requirements_012001.txt (last visited Oct. 22, 2001).
[8] Werdegar, *supra* note 2, at 105
[9] Kurt Wimmer, *Privacy and Mobile Telecommunications*, 19-SUM Comm. Law. 20, 22 (2001).

response to a wireline 911 call, thereby enabling emergency response personnel to address a call with the same speed and accuracy regardless of the type of telephone used.[10]

The final FCC regulations mandated that the conversion to E911 technology be accomplished in two phases. The first phase involved implementing the technology that would allow emergency personnel to automatically determine the cellular phone number of the caller and the location of the cellular tower receiving the call.[11] The wireless service providers completed this phase in June 2000. The second phase requires cellular telephone companies to deploy technology that would facilitate Automatic Location Identification (ALI), either through global positioning services or positioning determinations made through cellular telephone networks.[12] Each wireless service provider was required to come up with its own plan to implement the best ALI strategy given the company's existing technology and resources.[13]

While cellular telephone companies implemented the first phase with little additional cost, the second phase has proven to be quite expensive for the cellular providers.[14] The caller's telephone number and the location of the cellular tower receiving the call are data that the wireless service providers already collect to facilitate billings to customers.[15] However, according to the wireless service providers, Automatic Location Identification lacks consistent standards and available equipment, thereby resulting in astronomical implementation costs.[16] Phase 2 of the E911 implementation was scheduled to be completed by October 1, 2001, but shortly before the deadline, all of the major wireless service providers filed for extensions. The FCC has agreed to extend the implementation deadline to November 30, 2001, but will likely assess fines and other penalties if the wireless companies delay much past that date.

Privacy Concerns and E911

Consumer Privacy Issues

Since it is clear from the FCC regulations that E911 technology will be implemented, privacy groups have focused their concerns on the ways in which this technology will be

---

[10] Federal Communications Commission, *FCC Wireless 911 Requirements*, *at* http://www.fcc.gov/e911/factsheet_requirements_012001.txt (last visited Oct. 22, 2001)
[11] *Id.*
[12] *Id.*
[13] Federal Communications Commission, *Fact Sheet: E911 Phase II Decisions*, *at* http://www.fcc.gov/Bureaus/Wireless/News_Releases/2001/nwl0127a.txt (last visited Oct. 22, 2001).
[14] Werdegar, *supra* note 2, at 105.
[15] Werdegar, *supra* note 2, at 105.

implemented and have lobbied government agencies and technology manufacturers alike. In developing E911 technology, cellular technology manufacturers have demonstrated some sensitivity to privacy concerns. Users of telephones that are GPS-enabled may turn off the positioning capabilities at the press of a button. Similarly, cellular networks may restrict the use of the triangulation location method to situations where the caller has dialed 911; only in an emergency would the position of the cellular telephone be tracked. Through these technological advances, the cellular telephone networks and manufacturers have attempted to eradicate privacy concerns over E911.[17]

Despite the assurances of these cellular technology networks and manufacturers, privacy advocates remain concerned that the system originally conceived and designed to allow rescue workers to respond to emergencies will be pressed into other uses. Chief among these concerns is the perception that, with no clear privacy policies in place, retailers and specialty advertising and marketing companies are gearing up to take advantage of location information as soon as it is available from wireless carriers.[18] Other observers' worry that E911 will develop into an indiscriminate governmental surveillance system that would give Orwell nightmares.[19] Both of these fears appear to have some basis in reality, but it remains unclear whether the architecture of the E911 systems will make either Big Brother or Big Ad a reality.

While none of the major privacy advocates have come out in opposition to the commercial use of E911 location information altogether, most do have a problem with the way in which that information may potentially be used by advertisers and retailers. The primary issue here is control: will the user of the wireless service have ultimate control over whether and how his or her location information will be used, tracked and recorded?[20]

---

[16] Wired News Report, *FCC Grants Waivers on E911, at* http://www.wired.com/news/business/0,1367,47356,00.html (Last visited Oct. 5, 2001)

[17] *See* Richard Smith, *E911 Privacy Protections, at* http://www.privacyfoundation.org/commentary/tipsheet.asp?id=25&action=0 (last visited Oct. 22, 2001).

[18] *See* Comments of Evan Hendricks, *FTC Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues, "Location-Based Services and Advertising: Possibilities and Privacy Concerns", December 12, 2000, at* http://www.ftc.gov/bcp/workshops/wireless/001212.htm (last visited Oct. 22, 2001).

[19] Testimony of Deirdre Mulligan before the House Committee on the Judiciary, Subcommittee on Courts and Intellectual Property, March 26, 1998.

[20] *See In the Matter of Petition of the Cellular Telecommunications Industry Association for a Rulemaking to Establish Fair Location Information Practices*, Comments of the Center for Democracy and Technology before the Federal Communications Commission, WT Docket No. 01-72, DA-01-696, *at* http://www.cdt.org/privacy/issues/location/010406fcc.shtml (last visited Oct 22, 2001).

One key issue is whether a particular consumer's location information will be tracked in the first place.[21] The major concern for both advertisers and privacy groups is whether cellular telephone subscribers have the ability to opt-in or opt-out of participation in the location tracking system. With an opt-in choice, favored by privacy advocates, consumers would have to affirmatively choose to have their location information divulged to advertisers, which should theoretically mean that only consumers who actually want such information revealed will be part of the advertising pool. An opt-out option, obviously favored by advertisers, would make the consumer's location information available by default. Consumers would then have to contact their wireless carrier proactively if they were to decide that they no longer wished to share their information. Advertisers generally favor this alternative, knowing that relatively few consumers will take the time and effort to change their default status.

In addition to the basic question of whether consumers will have their location tracking shared with commercial services, concerns regarding anonymity and long-term information tracking and storage remain. For advertisers, functional anonymity may not turn out to be a deal breaker; for example, Burger King may like to know your real name when they send you the 10% off coupon as you drive past their store, but it will probably be sufficient for their purposes to know that you are inclined to eat at a variety of fast food restaurants when you are on the road and you are near one of theirs. So long as the wireless service provider or its advertising tracking service is able to generate a sufficient profile based on past preferences and location history, most advertisers will not need to know who that profile describes specifically.

Once a fully developed wireless location system matures, it seems likely that at least some consumer location information will be stored after the fact. The place where this information is stored also has the potential to seriously impact users' expectations of privacy. If location information were tracked within an individual's handset, for instance, then that information would be available to anyone who might subsequently find or steal the handset. If the information were stored on a long-term basis by the wireless carrier, then a hacker who manages to infiltrate their network security would have access to the records of tens of thousands of location histories. Furthermore, unethical wireless carriers might choose to use or sell this information at a later time, even if it means that they would be violating their privacy policy. As experience with Internet privacy policies in the last few years has shown, companies may not always respect the bargain that they make with their customers when economic conditions

---

[21] For a complete discussion of the opt-in/opt-out issue, *see FTC Workshop*, "Introduction to Privacy and Security Issues Panel", *at* http://www.ftc.gov/bcp/workshops/wireless/001212.htm (last visited Oct. 22, 2001).

necessitate change.[22] The Federal Trade Commission has made it clear that companies that renege on their privacy policies do so at their peril and that further regulation and litigation in this area are forthcoming.

In an effort to head off government regulation, several industry groups have been pushing for a self-regulatory structure "with teeth" that would protect consumers and ensure the widest possible latitude for advertisers to use location information.[23] Groups working to develop such a preemptive regulatory framework include the Cellular Telecommunications Industry Association and the Wireless Advertising Association. Both expressed their support for this self-regulatory proposal at a workshop held by the Federal Trade Commission on E911 issues in December 2000. While these initiatives are still in the embryonic stage, they illustrate that consumers and privacy advocates are not the only ones interested in addressing privacy issues. Many advertisers believe that they will be allowed greater latitude by the FTC and other governmental agencies if they self-police.

Unlike many governmental responses to new technology, the FTC, the agency most likely to be responsible for protecting consumer privacy once E911 is fully operational, has taken an active role in shaping and responding to the debate on wireless privacy. At last December's FTC Workshop, companies such as Nextel, Expedia and 24/7 Media all highlighted their sensitivity to issues such as consumer choice and privacy.[24] These actors seemed to realize that increasing consumer awareness of privacy issues might complicate their future plans if they do not address these problems early on.

There has also been a significant congressional response to the concerns over consumer privacy and wireless location technology. Representative Rodney Frelinghuysen (R-NJ) introduced a bill in January 2001, which would revise the Communications Act of 1934 to require informed customer consent to the provision of wireless call location information.[25] Similarly, Senator John Edwards (D-NC) proposed a new bill in July 2001, which would require consumer consent to the tracking of location information.[26] While these bills demonstrate that certain members of Congress are listening to the concerns of privacy groups, it is unlikely that much

---

[22] *See* FTC Press Release, *FTC Announces Settlement With Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations*, July 21, 2000, *at* http://www.ftc.gov/opa/2000/07/toysmart2.htm (last visited Oct. 22, 2001).
[23] *See* FTC Workshop, *Emerging Self Regulatory Issues*, *at* http://www.ftc.gov/bcp/workshops/wireless/001212.htm (last visited Oct. 22, 2001).
[24] *See* FTC Workshop, *The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, *at* http://www.ftc.gov/bcp/workshops/wireless/001212.htm (last visited Oct. 22, 2001).
[25] H.R. 260, 107th Cong. (2001).

emphasis will be placed on these measures given that Congress is presently focused on passing legislation to facilitate government surveillance.[27]

E911 Location Information and Law Enforcement Agencies

Although consumer interests may be adequately protected by a combination of congressional legislation, industry self-regulation and the FTC's active role, protections against unwanted intrusions by law enforcement and intelligence agencies may not have as many proponents, particularly in light of recent terrorist attacks in the U.S. While the contents of cellular telephone conversations remain protected under the standard set down by the U.S. Supreme Court in *Katz v. United States*,[28] at least one observer has noted that the use of cellular telephone location information by law enforcement would be more analogous to the use of pen registers or electronic tracking beepers, both of which have a lower evidentiary threshold than a true wiretap.[29]

Pen registers are devices that record the numbers dialed on a telephone line, allowing police to create a log of all outgoing calls from a suspect's phone. The use of such devices was upheld in *Smith v. Maryland*,[30] where the Supreme Court held that a telephone user did not have a reasonable expectation of privacy, one of the requirements of *Katz*, when he knew that the numeric information contained in the act of dialing would be sent to the telephone company.

Electronic tracking beepers are surveillance devices that are planted on a suspect which send out a signal detectable by police electronic equipment. In *United States v. Knotts*, the U.S. Supreme Court upheld the use of such tracking devices as constitutional, since they essentially only simplified a function that could be performed by more traditional surveillance methods, namely, following a suspect around.[31] When police use tracking devices to obtain information that would be unavailable by mere observation, however, the answer appears to be different. In *United States v. Karo*, an electronic tracking device that gave police information as to whether a container of material used to manufacture drugs was contained in a private residence was held to violate the Fourth Amendment.[32] The Court held that, since the information could not have obtained by the police using visual surveillance techniques, it crossed the line and constituted an

---

[26] S. 1164, 107th Cong. (2001).
[27] Elizabeth Douglass, Cell Phones Set to Track Call Locales, at http://www.latimes.com/technology/la-000082963oct18.story?coll=la%2Dheadlines%2Dtechnology (last visited Oct. 18, 2001)
[28] 389 U.S. 347 (1967).
[29] *See* Werdegar, *supra* note 2, at 103.
[30] 442 U.S. 735 (1979).
[31] 460 U.S. 276 (1983).

impermissible search. In the E911 context, since police would be able to use phone company records of past movements by a suspect which would be unavailable using visual surveillance techniques, it seems likely that the leniency given to the police in *Knotts* would not fully apply to cellular telephone location information.[33]

It has been suggested that part of Title III of the Omnibus Crime Control and Safe Streets Act, specifically 28 U.S.C. 2703, may provide some statutory protections against police use of cellular telephone location information.[34] Section 2703 provides protection for the electronic records of a telephone customer against seizure without a warrant. The Department of Justice released a memorandum opinion on the subject in 1996,[35] which states that electronic records concerning customer location information compiled by telephone companies should be subject to the same warrant requirements as other phone company records, meaning that police must show specific and articulable facts establishing reasonable grounds to believe that the information obtained is relevant and material to an ongoing criminal investigation. [36] The Department of Justice, however, stopped short of saying that this code section would apply to the use of location information outside the context of a 911 emergency call. In such situations, the legal standard required before the police could make use of cellular telephone location information remains murky. Given the general constitutional abhorrence of unfettered police power, it seems likely that the courts will impose a warrant requirement on use of location information; it remains to be seen, however, what standard will be used in granting such warrants.

Changes since September 11

In the immediate aftermath of the attacks on the World Trade Center and Pentagon, the privacy groups that had earlier expressed concern over the implementation of the E911 standard found that they faced two new factors in favor of the system. First, in the few days immediately following the attacks, some commentators believed that a fully functional E911 system would have aided rescue efforts. Second, as the U.S. commitment to the war against terrorism deepens, the need to track terrorists operating within the United States may lead intelligence and law enforcement officials to seek a greater degree of access to E911 tracking information than they would have needed before the attacks. Though neither of these new factors is unassailable, nor

---

[32] 468 U.S. 705 (1984).
[33] *See* Werdegar, *supra* note 2, at 109.
[34] *See Id*.
[35] *See Memorandum Opinion Issued By Department of Justice Concludes that Commission's Recently Adopted Wireless Enhanced 911 Rules are Consistent with Wiretap Act*, Fed. Comm. Comm'n, CC Docket No. 94-102, Dec. 10, 1996
[36] 28 U.S.C. 2703(c)(1)(B)

do they totally outweigh the important privacy considerations that have characterized the earlier debate, they do mean that privacy advocates will be forced to consider carefully any further objections to a system that seems to be in the national interest.

When the World Trade Center towers collapsed, burying thousands of people in the rubble, emergency workers began a feverish search for survivors. During the first few hours after the collapse, cellular telephone calls were received from numerous survivors trapped in the debris, with at least one rescue being attributed to a cellular telephone call.[37] While such anecdotes illustrate the need for E911 service, they also suggest that the urgency behind this need will continue to grow along with fears about further major terrorist activities. And any increase in the pace of deployment of the system is likely to lead to a sacrifice of privacy concerns in the interests of speed.

The value of an effective location tracking system during the current national crisis is also likely to cause privacy advocates great difficulty as they seek to slow the nation's plunge into the world of enhanced wireless location sensing. While in an ideal world, privacy groups would like location information to remain anonymous, law enforcement and intelligence officials are unlikely to share this view. Given the speed with which events are now unfolding both at home and abroad, a well reasoned, carefully considered approach to protecting privacy in the E911 system is likely to be an unfortunate casualty. The recent deployment of sophisticated electronic monitoring systems such as Carnivore and Echelon,[38] along with Congress' recent expansion of the wiretapping statutes, makes it more likely that law enforcement agencies will request that E911 location information is always on and always identifiable.

Conclusion

The current political situation in the United States has led to a shift in the balance of national security and privacy for many Americans. While most citizens might have found the notion that the government could potentially track the location of a cell phone to be frighteningly intrusive prior to September 11, many in the present climate would favor the implementation of

---

[37] *See* Ben Charny, *Could E911 Have Helped in Disaster?* ZDNet Asia News, 9/13/2001, *at* http://www.zdnetasia.com/news/wireless/story/0,2000024746,38014490,00.htm (last visited Oct. 22, 2001).

[38] For a description of these monitoring systems, *see Internet and Data Interception Capabilities Developed by the FBI*, Statement for the Record, U.S. House of Representatives, the Committee on the Judiciary, Subcommittee on the Constitution, 07/24/2000, Laboratory Division Assistant Director Dr. Donald M. Kerr, *at* http://www.cdt.org/security/carnivore/000724fbi.shtml (last visited Oct. 22, 2001); *see also ACLU Echelon Watch at* http://www.aclu.org/echelonwatch/index.html (last visited Oct. 22, 2001).

such a system irrespective of its toll on privacy. This is a precarious time to be introducing E911 technology, for it is unlikely that Americans will always be so willing to give up privacy rights in favor of tighter security. Hopefully, it will not be necessary to wait for the pendulum to swing in the other direction before privacy measures are integrated with the use of E911 technology.

The legislative measures still pending in Congress illustrate that the privacy groups' legitimate concerns over the protection of consumer privacy have not gone unnoticed. It is the responsibility of the sponsors of these bills to ensure that consumer privacy does not fall victim to the current focus on national security during this difficult time. If Congress is slow to implement these measures, it will be up to the wireless service providers to use technological solutions proposed by the cellular technology manufacturers to give cellular telephone subscribers more control over the use of their information. The most difficult balancing of privacy and national security concerns will be in the realm of government surveillance, where it still remains to be determined whether E911 data is subject to the same warrant requirements as other telephone record information. Above all, legislators and courts alike must remember that privacy should not and will not always take a back seat to national security; consequently, the balance, which is established during the implementation of the E911 infrastructure, will be critical to the technology's success in the years to come.

By: Aaron Futch
Christine Soares