The Ramifications of E911

Kristin Burke
Computer Science Department
Florida State University
burke@cs.fsu.edu
850.644.0058 (fax)

Alec Yasinsac
Computer Science Department
Florida State University
yasinsac@cs.fsu.edu
850.644.6407 (voice)
850.644.0058 (fax)

Abstract

With the advent of the new E911 system proposed by the Federal Communications Commission (FCC) new issues have been brought to the surface about whether these regulations will have negative ramifications exceeding the benefit of their positive ones. While the system's primary purpose is to locate cellular phone users who dial 911 in emergency situations, the ramifications of tracking abilities on cellular phone users lead to questions about future uses by law enforcement, private companies and market research firms. This paper discusses the possible ramifications of E911 on personal privacy, and some possible solutions to alleviate or reduce the problems.

1. Introduction

One of the most active technological growth areas in society today is in cellular telephones. Well beyond being simply mobile phones, their capabilities are only beginning to be uncovered. One recent proposal envisions developing a system that would allow government officials to determine the precise location of cell phones (and the user that possess them). There are many positive aspects of this capability; and many potential pitfalls.

In this paper, we present the background and technology that underlies location reporting capabilities associated with cellular service. We go on to detail some of the potential good and bad societal impacts that this technology presents, and propose solutions for some of these pitfalls.

2. Background

The popularity of wireless mobile communications is growing rapidly. In 1999, an estimated 48% of all adults owned a cell phone and in the year 2000 that number grew to 55% [SHA02]. The number continues to grow. As of June 5, 2002, CNN reports that the number of cell phone users in the United States is 137 million and by the year 2007 Americans will spend an average of 465 billion minutes on their cell phones each year [PAW02]. With numbers like those, it is reasonable to assume that some of those minutes are bound to be spent calling 911 emergency services.

In the year 2000, the National Emergency Number Association (NENA) estimates that of the 150 million calls that were made to 911 emergency services, 45 million of those calls were from cellular phones [BON02]. NENA estimates that this number will grow to more than 100 million by 2005. With this high percentage of calls coming from wireless phones, the Federal

Communications Commission (FCC) decided to take action to make wireless services more like the wired ones already in place.

In 1996, the FCC proposed regulations called “E911”, or enhanced 911 [CHA01]. These proposed regulations require wireless providers to automatically deliver the phone number and location of cell phones that called emergency services to the 911 operator. This paper outlines these regulations, the ramifications of them, some problems and issues with these ramifications, and offers solutions to alleviate some of the problems.

2.1. Cellular Communications Technology

In wireless mobile communications there are two main entities: the cellular phone and the network [PAR97]. The fixed cellular network consists of base stations (one in each cell), base station controllers, and mobile switching centers. The cell phone accesses the network by communicating directly with the base station in the nearest cell. The base station controllers manage the base stations and the mobile switching centers manage the base station controllers and the communication between the mobile network and other networks.

In order to communicate using a cellular phone, the phone and the network must share authentication information. When a cellular phone is first turned on, the phone sends an authentication request to the network in the form of a unique number. This allows the network to confirm that the particular phone actually belongs on the network and that an account exists.

After authentication, communication consists of two cellular phones (or a cellular phone and a phone on land) communicating through the use of a base station(s) and the network. The cell phone sends its information through radio signals to the nearest base station. The base station will decrypt the information, do some transformations and then the information is encrypted and forwarded to the other entity.

2.2. Enhanced 911

In 1996, the Federal Communications Commission proposed a system called Enhanced 911 (E911) [CHA01]. This proposal required all wireless communication carriers to eventually have the ability to report the location and telephone number of any person calling emergency services from a cellular phone. The caller’s longitude and latitude must be identified within 50 meters for 67% of emergency calls and within 150 meters for 95 % of the calls [CRO01]. These requirements are to be fulfilled by 2005.

The first phase of the E911 system began in April of 1998 and ended in October of 2001, with the exception of the extensions requested by most wireless communication carriers. During this phase, upon the completion of a call from a cellular customer to 911, wireless carriers were required to provide both the caller’s phone number and the location of the cell cite receiving that call to Public Safety Answering Points (PSAPs) [FCC02]. The second phase of the E911 system, to be completed by 2005, will provide the PSAPs with the first phase information, plus the location of the cellular caller to within 50 to 300 meters [CRO01].

There are several possible technological approaches for identifying the location of a cellular customer. In the following subsections, we detail these technologies.

2.3. Location Based Service

For the majority of wireless providers, location information will be acquired by a Location Based Service (LBS). LBS provides the “ability to find the geographical location of the mobile device and provide services based on this location" [PRA02]. There are several ways that a Location Based Service can find the location of a device, including both handset-based and network-based techniques. Some of these techniques include: Cell of Origin (COO), Time Difference of Arrival (TDOA), Angle of Arrival (AOA), Enhanced Observed Time Difference (E-OTD), and Network Assisted GPS (AGPS).

2.3.1. Cell of Origin

Cell of Origin is a network-based technique (i.e. the location information is determined by the network as opposed to the phone itself) may be used to find the phone that originated a call [CEL02]. For this service, the base station that routed the call is used as the location of the caller. The accuracy of this method is not high and depends upon the cell area [PRA02]. It may be as accurate as 100 meters (urban areas) or as erroneous as 30 kilometers [CEL02].

COO is inexpensive to use, as it requires no extra hardware to implement. Also, COO is fast, generally taking only a few seconds to associate a caller with a certain cell. While these two characteristics make COO favorable to the wireless carriers, Cell of Origin will only satisfy the first phase of the E911 system, since it is an inaccurate system. Therefore, COO must be accompanied by other location methods.

2.3.2. Time Difference of Arrival

Time Difference of Arrival (TDOA) is also network-based, yet instead of using one signal from a single base station it uses the differences in the times of arrival of several signals from the mobile phone to several base stations that are in the phone's range [PRA02]. These times are used to calculate the distance of the cellular phone to each base station, thus calculating the location of the cell phone itself. A wireless carrier needs at least three times of arrival from different base stations in order to calculate an accurate TDOA value [BIR99].

TDOA uses special transmitters, receivers and radio frequency (Rf) signals (more than just needed to transmit calls) [SCH01]. Location receivers are also used to capture the times of arrival of signals from the cellular phone at the different base stations. These location receivers translate these times into longitude and latitude and then the carrier then forwards this information on to the PSAP. TDOA is shown in Figure 1 as taken from [TDO02]

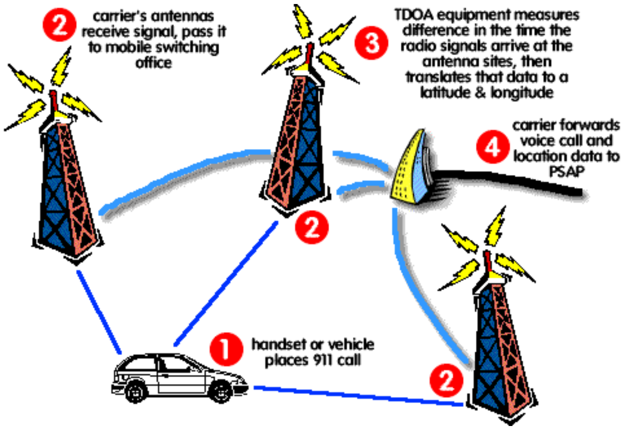
2
carrier's antennas receive signal, pass it to mobile switching office
3
TDOA equipment measures difference in the time the radio signals arrive at the antenna sites, then translates that data to a latitude & longitude
4
carrier forwards voice call and location data to PSAP
2
1
handset or vehicle places 911 call
2

Figure 1

Although these items will create new expenses for cellular companies, the greatest expense of this technique is the need for synchronization of the cellular network. This type of synchronization requires the accuracy of atomic clocks at each base station, which, at the cost of upwards of $50,000 [BH02], may not be a feasible goal.

2.3.3. Angle of Arrival

Angle of Arrival (AOA) is a network-based technique that uses at least two base stations to measure the angle of the incoming transmission from the cell phone [BIR99]. With these two angle measurements, the approximate location of the phone can be calculated through a combination of time of arrival and simple geometry.

AOA requires a complex array antenna and cables at each base station. Location receivers, much like in the TDOA system, are also needed to relay the angle data back to the network for calculation. While AOA is a feasible method for wireless providers to comply with E911, some carriers may not desire to put forth the money necessary to supply antennas and location receivers at every base station. Many carriers will instead move on to the Assisted Global Positioning System method, which requires less equipment and is more accurate than AOA.

2.3.4. Global Positioning System

The Global Positioning System (GPS) is a handset-based technique that is growing in popularity for its accurate location measurements. This system works through the use of the GPS satellite constellation, which was deployed by the United States Government beginning in 1986 [GPS02]. These satellites orbit the earth twice a day while they transmit both their position and elevation. The GPS receiver acquires a signal from at least three satellites and measures the interval between each satellite’s transmission and the receipt of the signal. This data is used to calculate the distance between each satellite and the receiver. All of these distances, when drawn in sphere-like fashion around the receiver will intersect at exactly one point. This point is the location point of the receiver. This concept is shown in Fig. 2 as taken from [BH02].

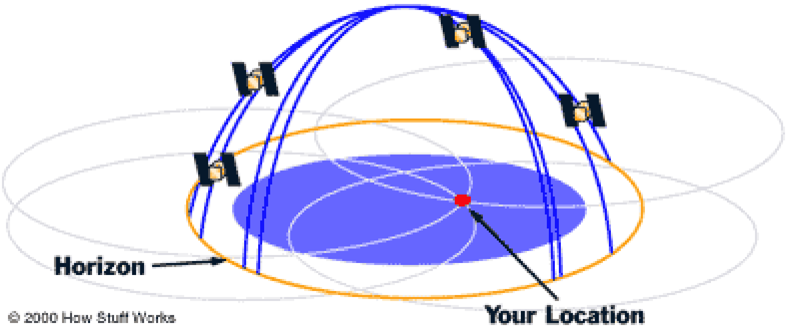

Fig. 2

In order to use GPS, each cell phone would have to be equipped with a GPS receiver, which is an added cost to the system. Wireless providers choosing to use this method may either cover the added costs themselves or add the costs to the regular monthly service fees charged to users [CRO01]. Also, users may have to buy new phones in order to comply with the E911 regulation.

2.3.5. Network-Assisted Global Positioning System

Network-Assisted Global Position System (AGPS) is a technique based on GPS. AGPS requires partial GPS receivers in every mobile station [DR01]. The network would need to be running an AGPS server with a reference GPS receiver that can “see” the same satellites that the receiver sees and at the same time. These two requirements allow the network and the handset to work together to find the location of the mobile station.

The network can predict the GPS signal that the mobile station is to receive, while the mobile station can correctly use weaker signals than a conventional GPS receiver. These characteristics, plus the fact that the network does the location calculations, allows a less expensive version of a GPS receiver to be required in the handsets, thus reducing the overall cost of the system.

AGPS is accurate to within 100 meters indoors and 15 meters outdoors, making it the most accurate method of locating mobile stations proposed thus far [DR01]. With the AGPS server and the GPS receivers being the only hardware necessary for implementation, it is likely that cellular companies will widely use AGPS to comply with the E911 requirements.

Although wireless companies may use one or any combination of these services to comply with the E911 regulations, because of the accuracy of GPS and AGPS, these are most likely the systems that will be used. Based on this assumption, in the sections to follow the negative ramifications of these systems, as used to satisfy E911 requirements, will be discussed. Section 3 is devoted to the ramifications on mobile subscribers through the use of GPS (hereby referring to both GPS and AGPS) in mobile communications. Section 4 deals with problems and issues of these ramifications arising from the use of GPS. Section 5 proposes some solutions to these possible problems and issues. Section 6 summarizes and concludes the paper.

3. Potential Ramifications on Personal Privacy

With the added ability to locate a cellular phone user with LBS comes concerns about how this data will be used. Although E911 only requires wireless providers to provide the location of mobile stations upon the completion of a call to emergency services (911), the providers themselves have already expressed a desire, and have plans in the works, to use this data for other purposes [GOL00]. This accumulated location data can be stored by the cellular providers for future use or shared with market research firms. All major cellular carriers now have plans to reveal cellular user location data to third-parties.[CRO01]

3.1. Data Mining and E911

Data Mining, also called Knowledge Discovery, can be defined as the “non-trivial extraction of implicit, previously unknown, and potentially useful information from data” [PRY02]. Data mining takes large amounts of data, known as data warehouses, and finds patterns in this data through statistical, visual or algorithmic search. Data mining has long been considered a threat to personal privacy because of its capability to extract personal information by combining large amounts of data that are otherwise considered to be benign.

Data mining is used by businesses to find patterns in customer behavior. For instance, Amazon.com uses data mining to produce “recommendation” products for their customers based on previous buying patterns [ama02]. Jiffy Lube uses data mining to find out which customers are likely to respond to mail-outs and then sends these customers reminders for different products and services [CSF01].

Harmless as it may seem, data mining can also be used for underhanded practices. Not too long ago, Macy’s was accused of using data mining on the private information of couples using the wedding registry system, and their guest’s purchases, in order to send advertisements to these people and send statistics about this information to other companies [EEF01]. Also, banks are now planning to use data mining to “weed-out” customers that are not profitable and to deny service to people based on statistics from their income, education and employment history. Many people could be denied service based solely on the practices of others with the same characteristics [EDW99].

Much in the same way, wireless providers can contract out their location data to third parties that conduct the data mining processes and find out much more information about cellular users through this data. For instance, marketing firms can find out where one spends most of his or her time: at home, on the road, shopping, etc. and can make judgments about people according to this data. Much like in the bank example, if a mobile user spends a large amount of time in a relatively bad section of a town, and law enforcement finds patterns in the data of those who spend time in this part of town related to criminal behavior, it is likely that this mobile user will be stereotyped as such.

This may lead to serious threats against one’s personal privacy and the privacy of society as a whole. While in most cases of protecting one’s privacy the particular person has the knowledge that privacy may be violated and can take steps to prevent this from occurring, in the case of data mining and the following examples, many people may be completely unaware that these abuses may occur. This leaves the public vulnerable to having personal information (including location information) used in ways that violates the right to freedom of movement.

3.2. E911 May Enable Location-targeted Advertisements

The main attraction for wireless providers to share or sell location information to third parties is the economic benefit that they may attain by providing that information for use in location-targeted advertising [CRO01]. Some of these advertisements would require monitoring the location of callers at all times, something the wireless companies have already agreed to do [GOL00]. The vendors wishing to advertise would use the location information to send notices to the mobile station when a cellular customer is approaching an entertainment attraction, store, restaurant, or other advertised service.

Location-targeted advertising can lead to a bombardment of advertisements to the mobile station. If a wireless provider shares the location information with too many third parties, cellular users could be getting notices from many vendors wishing to sell their wares. Compared to the current situation with cellular phones being almost completely private, cell phones will become the welcoming entity of spam. Much like the public is annoyed by email spam, cell phones may be the telephonic equivalent.

3.3 Misuse of Location Information

Besides the prospective annoyance, the actual sharing of information can lead to a problem. Not only will the wireless provider know a cellular users minute-by-minute location, but if the location information is shared, third parties will know too. This can lead to problems with privacy advocates who believe that this information is too private to be shared.

Location information can tell who stays at home much of the time, who travels a great deal (thus, whose house might be empty at any given time), and at what locations a person spends most of his or her time. This information can be considered private, or at least sensitive, as Americans feel free to go where they choose when they choose without the thought that this information might be recorded. This information as such should be shared with other companies or groups without the express permission of the tracked person.

3.4. Law Enforcement Tracking

Once wireless providers can gather the cellular location data, law enforcement agents may gain access to this information [CRO01]. Such location information can be useful to law enforcement for crime prevention and investigation, but there may be a negative societal impact of routinely providing this information to law enforcement authorities. While our constitution does not explicitly protect personal privacy, we are expressly protected from excessive search and seizure. Gathering location information can become threaten this right.

3.4.1 Using Location Information for Traffic Ticketing

Although usually overlooked, GPS and AGPS receivers will also track the velocity at which the mobile station is moving in addition to the location and altitude if four satellites are employed [EP99]. Thus, law enforcement agencies may use location tracking to discover if cellular users are traveling at a higher speed than the speed limit of the street/highway on which they are traveling. Some may champion this technological breakthrough as a mechanism for saving lives and fuel. Others may see it as an unwelcome intrusion and a violation of excessive search and seizure.

With political arguments aside, are their technological problems with using E911 as an extra-terrestrial speed trap? One issue is: "How the cell phone be connected to the driver?" While it may not be wise, it is not illegal to ride with a speeding driver, nor is it illegal to loan a cell phone to a speeding driver.

A second issue relates to billing. Since the phone number will tie the violation to the cellular owner, will the ticket amount be charged to the cellular account? The possibilities are unlimited. If the violation is minor, law enforcement could simply call the owner and tell them to slow down.

There are also issues of accuracy of the GPS system, both in measuring velocity and in tracking the signal to the proper cellular user.

Even if all these issues can be resolved, the question of improper search and seizure must be addressed. Authorities must acquire a warrant to legally intercept communications. Existing law must be reviewed and updated to protect against abuse of location information.

3.4.2 Following Criminal Behavior

If the owner of a cellular phone is suspected of a crime, it is likely that law enforcement could use the location data of the mobile station to track the person. This can be a useful tool, much like phone wiretapping, to find out whom this person is having communication with or visiting often. If the cellular user is suspected of something more malicious, such as murder, it is probable that past location data may help to provide evidence as to the person’s alibi and contacts.

While these are useful tools, if left unchecked the power they provide may lead to corrupt use. For instance, unwarranted tracking could take place, which means that innocent people would be tracked for no apparent reason, or would be suspected of crimes simply based on their location at a particular time.

4. Manifestation of E911 Side Effects

Many problems arise when technology is used in unintended ways. Having discussed the ramifications of implementing E911, what follows are some of the problems and issues that arise from these ramifications.

4.1. Outraged Public

One issue that may arise from the advertisements, data mining, ticketing, etc. is public outrage. At this time two-thirds of Americans desire to have location-based services in their mobile phones [PAR02]. This desire is based on the assumption that the services are helpful to the cellular customer for safety reasons. While there are personal safety benefits to the LBS, such as roadside assistance and location in emergencies, many of the negative ramifications are currently unrecognized by the public. It is probable that upon the realization of these ramifications, the public will not be pleased.

This outrage has not occurred as of yet, and this information will not likely be available to the public until after E911 is put in place resulting in a retroactive response similar to the anger of the “TiVo outrage” that occurred in 2001 [MAR01].

The TiVo service was created in 1999 and allows viewers to record TV programs or certain types of programs for later viewing [MAR01]. There was an initial cost and a monthly subscription fee, and the public thought this was a wonderful invention. By January 30, 2000, TiVo had 154,000 subscribers and was growing fast. TiVo executives even made statements about using the service to provide targeted advertising to viewers.

The outrage ensued soon thereafter. In March of 2001, The Privacy Foundation released a report on the privacy issues surrounding TiVo; outlining how TiVo tracked every channel change, program watched and program recorded and then transferred this information to its headquarters to be deposited in a database [MAR01]. When the public was exposed to this report, many people were outraged over how their private viewing information was being handled by TiVo.[MAR02] This led to TiVo apologizing and prompting the public for advice on how to better handle the information

While TiVo escaped this embarrassment without losing too much of their customer base, the risk that was taken was great. It is a viable assumption that TiVO did not go out of business only because the benefits of the product outweighed the privacy costs and mistrust of the consumer. Will this be the case for cellular companies and E911? Will location technologies need to provide more to the consumer in order for the customers to be assuaged?

4.2. E911 and Cellular Fraud

Cellular Fraud is classified as the “unauthorized use, tampering, or manipulation of a cellular phone or service”[CON02]. It was a misdemeanor until 1993, after which time it became a federal crime [BAC96]. The cellular industry estimates that “more than $1.5 million a day in revenue is lost to fraud, despite efforts to detect and prevent it”. There are four types of cellular fraud, two of which will be highlighted in this paper: cellular cloning and subscriber fraud.

Cellular cloning involves an attacker illegally monitoring radio waves and picking up Electronic Serial Number (ESN)/telephone number (MIN) pairs when they are being transferred to the network to initiate service [CON02]. The attacker can make the network believe that their phone is the victim’s and, as a result, all calls made on the clone are charged to the victim [BAC96].

Subscriber fraud involves an attacker illegally obtaining the private information of another individual through some means and using that information to open a cellular account [CON02]. It may take a long time to discover subscriber fraud and the recovery process is arduous for the victims. Subscriber fraud can ruin a victim’s credit, which is a difficult error to correct.

Another side effect of location tracking technology is that it may cause a significant rise in the volume of cloning and spoofing that occurs. It is likely that criminals would engage in both of these types of activities more often if there was a risk of being tracked by law enforcement through a legitimate phone.

This becomes an even bigger problem because the act of fraud may cause even more problems, such as incorrect ticketing and mistracking.

4.3. Incorrect Ticketing

Incorrect ticketing may occur when cellular fraud is taking place through cellular cloning or subscriber fraud. The situation may arise that an attacker would be in possession of a phone that is linked to an account in a different name. If law enforcement employs the ticketing system then incorrectly ticketing cellular customers could occur.

While this may not seem like a problem of large magnitude, it can quickly become one. Let us say for instance that an attacker clones a person’s phone. Now both the attacker and the victim have the same cellular account. Not only are both entities making calls, but also one account is being charged for those calls. In addition, one account is being charged for moving violations as well. In the event that the attacker is not a safe driver, this account can be charged for speeding tickets as well. This can add up to a large bill and a large headache for the victim.

4.4. Mistracking

Mistracking may occur when an attacker commits cellular fraud and then uses the cloned mobile station to commit a crime. After this crime is committed, the attacker can then shut off the cloned phone and the only phone being tracked by law enforcement would be the legitimate cell phone. This could cause wasted tax dollars to track innocent people and could cause victims unneeded suffering.

These attacks may be able to occur because there is no distinct relationship between the GPS receiver and the ESM/MIN pair. Cellular phones can be cloned and if the clone has a GPS receiver, it is automatically associated with the ESM/MIN. This may not seem like such a problem if accounts are constantly monitored so that there are no duplicates being tracked, but with the amount of cellular customers this monitoring seems unlikely.

4.5. Attacks on GPS

In addition to the attacks on cellular location information uses, it is a good probability that there will be increased attacks on the Global Positioning System itself to try to subvert the tracking abilities. Also, with more people using GPS and more focus on the system, attackers are, in general, more likely to attempt attacks. There are three main types of attacks on a GPS system: spoofing, jamming and meaconing [DEJ02].

4.5.1. Spoofing

Spoofing occurs when an attacker uses a technical device to simulate false GPS satellite signals.[DEJ02] This causes the receiver to lock on to this signal and, as a consequence, receive a false measurement for location. The U.S. Military took care of this problem for the government-only satellite broadcasts in 1994, but the problem still remains for civil GPS use.

This attack would likely only occur as a result of malicious behavior rather than an attack on tracking or location-based services. While in a regular GPS system this attack would render the location services unusable, with AGPS this attack would likely do no harm. This is because the AGPS receiver in the phone has a back up in the AGPS server on the network to find its location.

4.5.2. GPS Jamming

Jamming is producing intentional radio frequency interference with the express purpose of blocking the GPS satellite signals to receivers [DEJ02]. Jamming is achieved by an attacker through the use of an inexpensive and easily attainable device called a jammer. Jammers are readily available on the Internet and can cause receivers from up to 1000km to receive no signals from satellites to generate a location. Attackers may use jamming to subvert mobile station tracking capabilities. This includes law enforcement tracking and E911 emergency services.

4.5.3. Meaconing

Meaconing is the act of receiving, delaying and then rebroadcasting old GPS satellite signals to confuse GPS users [DEJ02]. Much like the spoofing attack, it is simply a malicious attack that may increase in frequency if GPS is used as a law enforcement approach.

5. Proposals

In this section, we propose solutions to some of these issues, problems and ramifications.

5.1. Public Announcements to Reduce Societal Stress

One way to alleviate the possible public outrage is to make the possible negative ramifications of E911 public. For instance, law enforcement tracking and ticketing, advertising and data mining should be explained to people and noted as possibilities that might stem from the new location-based services. This way, people can have a choice to turn off their phones if they want total privacy.

With this revelation, more people will be able to scrutinize the way that location-based services are working and may be able to alleviate some of the problems through technology. Also, legal professionals would be able to measure the constitutionality of some of the law enforcement aspects of the services. The more people that are able to examine all possible consequences of E911, the more likely successful solutions to these problems can be created. In addition, of course, this would allow cellular users to turn off their phones if they desired their privacy at any time.

5.2. Value-added Incentives for E911

In order to curtail possible anger over ramifications or monetary expense associated with the new E911 regulations, it may be practical for wireless providers to offer supplemental benefits to cellular users that choose to employ E911. It would be simple for wireless providers to equip every mobile station with a GPS receiver and use that receiver only for location purposes within the network. It would, however, be a benefit to the cellular customer if other GPS services were offered.

For instance, stand-alone GPS receivers allow the user to find his or her own location using the GPS satellite constellation. This is beneficial for long trips, outdoor sports or general navigation. Most of these receivers also have maps included in order to provide a more accurate location and navigation service for the user. If these services were included with the mobile station, it is likely that the cellular customer would be less agitated about possible ramifications stemming from E911.

5.3. User Authentication Using PINs

It has been previously suggested that Personal Identification Numbers (PIN) numbers should be used with cellular phones in order to curb the problem of cellular fraud [PAR97]. These numbers prevent fraud by working as a personal identifier for the owner of a cellular phone. The PIN could be used at the initiation of cellular service when the mobile station is powered on, as the PIN is only known by the user and therefore only the user could send the PIN to the network. After the network verified the PIN, the user could then engage in cellular communication.

Personal Identification Numbers were actually available as a service for cellular phones in the mid-1990's. [BAC96] One of the reasons that this idea may not have caught on was the relatively low occurrence of cellular fraud and the limit on possible monetary loss due to fraud. With the advent of law enforcement ticketing, however, it is much more likely that high cellular bills due to fraud can be generated.

This phenomenon makes it even more imperative to protect cellular customers from fraud. Not only does a GPS receiver in the mobile station make it more personally identifiable to the user (through advertisements, previous location data), but the receiver also makes the account more vulnerable to higher monetary obligation due to fraud. PIN utilization could also help to control mistracking due to fraud.

5.4. Allow Cellular Users to Opt-out of Location Sharing

Allowing cellular customers to opt-out of certain services may also help to quell outrage over the sharing of location information to third parties. Customers should be given options about whether their information should be used in advertising and data mining. When given a choice, customers are more likely to feel better about the situation and are unlikely to actually opt out. As capricious as that may seem, it is human nature. Give the option and the customer may not take it, but will appreciate the fact that it was offered.

5.5. Enacting Suitable Laws to Support E911

In order to make the public feel secure that their information is not being mishandled and that they are not being tracked in an unconstitutional manner, laws need to be proposed to ensure the protection of civil rights. These laws need to address the release of location information to third parties, the requirements for a warrant before law enforcement can get location information and the misuse of the location information by third parties.

6. Conclusion

Despite its problems, E911 and location-based services can serve many purposes. In safety aspects, roadside assistance and emergency services are aided enormously by the location information provided by these services. If a cell phone is lost or stolen, the LBS can almost work as a sort of “LoJack” for finding the phone again; if the new possessor turns on the phone, he can be located immediately. These services alone are worth some problems with the rest of the system.

These problems, however, if unchecked can escalate into the public having to give up personal freedoms for these services. Tracking, data mining, and over-advertising can cause many more hardships for the customer than the safety services are worth. For this reason, these ramifications of E911 must be openly discussed, researched and alleviated. Otherwise, there may be many more problems on the horizon than this paper could ever anticipate.

In this paper, we give the societal requirement and technical background for location discovery through the cellular telephone system. We addressed many of the fundamental characteristics of such service and addresses several associated, negative unintended side-effects. Finally, we proposed solutions to some of these problems.

E911 and the associated technology has tremendous potential to benefit society. As a responsible society, we must ensure that the positive results do not blind us to the potential threats that may be posed by the side effects of this technology.

7. References

[ama02] www.amazon.com <http://www.amazon.com/exec/obidos/tg/browse/-/508506/ref=hp_hp_ls_3_2/002-2271693-7267232>

[BAC96] Backer, Noelle. "Are Techno-Criminals Stealing the show?" The Crafts Report Apr. 1996. 6 June 2002 <http://www.craftsreport.com/april96/cellularfraud.html>.

[BER02] Berry, Sharon. "Quirks in Nature Enhance Global Positioning System." SIGNAL Jan. 2002: 1-3.

[BIR99] Birchler, Mark. E911 Phase 2 Location Solution Landscape. 28 June 1999. Motorola Labs. 10 June 2002 <http://www.fcc.gov/realaudio/e911mot.ppt>.

[BON02] Bonsor, Kevin. "How Location Tracking Will Work." How Stuff Works. 9 June 2002 <http://www.howstuffworks.com/location-tracking2.htm>.

[BH02] Brain, Marshall, and Tom Harris. "How GPS Receivers Work." How Stuff Works. 9 June 2002 <http://www.howstuffworks.com/gps.htm>.

[CEL02] "Cell of Origin." Search Networking.com. 10 June 2002 <http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci509920,00.html>.

[CHA01] Charny, Ben. "Could E911 have helped in disaster?" CNET News.com 12 Sept. 2001. 24 May 2002 <http://news.com.com/2100-1033-272923.html?legacy=cnet>.

[CHR01] Christensen, Gerry. Mobile Positioning. 2001. 10 June 2002 <http://www.mobilein.com/mobile_positioning.htm>.

[COM01] Compaq Computer Corporation. "Compaq Streamlines Location Services." Wireless Developer Network 27 Mar. 2001. 29 May 2002 <http://www.wirelessdevnet.com/channels/wireless/features/compaqfcc911.html>

[CON02] Consumer Alert: Cell Phone Fraud. 25 Mar. 2002. Federal Communications Commission. 6 June 2002 <http://www.fcc.gov/cgb/consumerfacts/cellphonefraud.html>.

[CRO01] Crouch, Cameron. "Analysis: Will Big Brother track cell users?" CNN .com 3 Aug. 2001. 24 May 2002 <http://www.cnn.com/2001/TECH/ptech/08/03/911.cell.tracing.idg/>.

[CSF01] Case Study Forum, Data Mining. 12/31/2001, Aug. 7, 2002 http://www.ecomlink.org/E_incubator/Case_Studies.asp?CategoryID=676#2

[DEJ02] De Jong, Kees. "GPS Limitations and Vulnerabilities." GeoInformatics Apr. 2002. 6 June 2002 <http://www.geoinformatics.com>.

[DR01] Djuknic, Goran, and Robert Richton. "Geolocation and Assisted GPS." IEEE Compute Magazine Feb. 2001. 10 June 2002 <http://www.cs.huji.ac.il/~postPC/Geolocation_assistedGPS.pdf>.

[EDW99] Edwards, Lynda. “Big Banker is Watching.” Bankrate.com. 22 Jan. 1999. Bankrate.com. 14 Mar. 2002 <http://www.bankrate.com/brm/news/bank/19990122.asp>.

[EEF01] EEF Alert: Macy’s & Your Privacy 6/5/01, Aug. 7, 2002. <http://www.eff.org/Privacy/Marketing/20010612_eff_macys_alert.html>

[EP99] Eng, Per, and Misra Pratap. “Scanning the Issue/Technology: Special Issue on Global Positioning System.” Proceedings of the IEEE 87.1 (1999): 3-15.

[FCC02] FCC: Enhanced 911. 23 May 2002. Federal Communications Commission. 24 May 2002 <http://www.fcc.gov/911/enhanced>.

[GOL00] Gold, Steve. “Privacy Storm Brewing Over Mobile Phone Location Technology.” Computer User. com 13 Nov. 2000. 10 June 2002 <http://www.computeruser.com/news/00/11/13/news14.html>.

[GPS02] GPS History. 2001. 28 May 2002 <http://www.safetrack.com/History.htm>.

[INF02] Infowar.com. Commentary on GPS and Trusted Time Sources. 6 June 2002 <http://www.infowar.com/chezwinn/articles032000/GPSCommentary.shtml>.

[MAR02] Martin, David. Court orders SONICblue to develop and deploy spyware for Big Media. 31 May 2002. 9 June 2002 <http://www.cs.bu.edu/~dm/pubs/replaytv.html>.

[MAR01] - - -. TiVo’s Data Collection and Privacy Practices. 26 Mar. 2001. 10 June 2002 <http://www.privacyfoundation.org/privacywatch/report.asp?id=62&action=0>.

[MCG02] McGeough, Jim. “Location-Based Services and Topology.” GeoCommunity 27 Dec. 2001, Originally published and presented at the GITA conference, Aug. 29, 2001 ed. 29 May 2002 <http://spatialnews.geocomm.com/features/geomode2/>.

[OAK98] Oakes, Chris. “’E911’ Turns Cell Phones into Tracking Devices.” Wired News 6 Jan. 1998. 24 May 2002 <http://www.wired.com/news/technology/0,1282,9502,00.html>.

[OAK99] - - -. “Zeroing In on Cell-Phone 911s.” Wired News 30 June 1999. 24 May 2002 <http://www.wired.com/news/technology/0,1282,20504,00.html>.

[PAR97] Park, Chang-Seop. “On Certificate-Based Security Protocols for Wireless Mobile Communication Systems.” IEEE Network. September 1997.

[PAW02] http://www.cnn.com/2002/TECH/ptech/06/05/toxic.cell.phones/

[PFE02] Pfeiffer, Krista, Eric Papacek, and David Smith. Data Mining Privacy Problems. 14 Mar. 2002 <http://www-personal.umd.umich.edu/~kpfeiff/problems.htm>.

[PRA02] Prasad, Manish. Location Based Services. 28 May 2002 <http://www.gisdevelopment.net/application/lbs/lbs002pf.htm>.

[PRY02] Pryke, Andy. The Data Mine. 10 June 2002 <http://www.the-data-mine.com/bin/view/Misc/DataMining>.

[SHA02] http://www.shanemedia.com/article.asp?articleID=326

[SCH01] Schutzberg, Adena. Making Sense of Location-Based Services. 15 Nov. 2001. Ultimate GIS Directory. 28 May 2002 <http://www.tenlinks.com/mapgis/articles/comment/111501LBS.HTM>.

[SNA02] SnapTrack. Hybrid Wireless Assisted GPS Provides E911 Public Safety. Jan. 2002. 10 June 2002 <http://www.nena.org/Wireless911/CIF%20Presentation%20PDFs/Chris%20Verbil.pdf>.

[TDO02] TDOA Location Technology, Dispatch Monthly Magazine. 6/29/02 Aug 8, 2002 http://www.911dispatch.com/911_file/tdoa.html

[WIL02] Willen, Claudia. “Airborne Opportunities: FCC push to finalize E911 capablilities spurs location-based product development.” Intelligent Enterprise 14 Jan. 2002. 29 May 2002 <http://www.intelligententerprise.com/020114/502news3.shtml>.

[WRO01] Wrolstad, Jay. “Verizon Wireless Launches E911 Phone- Service to Follow.” Newsfactor Network 27 Dec. 2001. 28 May 2002 <http://www.newsfactor.com/perl/story/15514.html>.

[YAP02] Yap, Steve. Mobile Positioning Technologies. 10 June 2002 <http://www.ida.gov.sg/Website/IDAContent.nsf/dd1521f1e79ecf3bc825682f0045a340/ecc486d188604008c825698900089fed/$FILE/positioning.pdf>.