The Ethics of Personal Privacy and Location-Based Services

By Kellie Kuebler, David Palm, and Auburn Slavec

Personal Privacy is being compromised by the intrusiveness of location-based services and its exposure of personal information to third parties.

It is Friday and your workday has finally come to an end. Soon your incoming calls will be invaded by open invitations to the events of the evening. Once everyone is piled into your conservative four-door, you’re off to the bars. Finally, you’re at the first club. Working your way to the bar, the crew is looking around for anyone they know, or would like to know. As the night goes on, it has been three hours and you still haven’t left that bar. You decide it is time to leave. After finally getting your friends into the car you take off only to be stopped one block away from the bar by a patrol car. You are issued a sobriety test but you haven’t had a drink all night; you were the designated driver. The device in your vehicle alerted the police and your insurance company of the duration you spent at the bar. You may pass the test with no problem, but that won’t help the outrageous increase of your insurance rates as you have now been deemed a high risk driver. As extreme as it may sound, it is not that far fetched. In fact, insurance companies are currently looking into the pay-as-you-drive program in which rates would fluctuate depending upon each customer’s risk evaluation. Such evaluations could legally be determined by monitoring the location-aware device installed into vehicles.

Modern day technology has resulted in the emergence of location-based services (LBS). LBS are applications that use information about where a communication device is located. Location information has the potential to allow an adversary to physically locate a person, and therefore most wireless subscribers have legitimate concerns about their personal safety if such information should fall into the wrong hands. These services can range from the GPS chips in your mobile devices to the Emergency services in your car. At any time your past and present location can be pinpointed down to a few centimeters just by accessing your account information.

Location-based services create an ethical dilemma in three different ways. First, the potential for misuse is too great to ignore and as the technology becomes easier to use, the good possibilities do not outweigh the bad. Another ethical dilemma created by LBS is that it compromises our duty to respect each other and treat one another as we would like to be treated. LBS provide an opportunity to consistently be aware of where someone is going and as a result they create suspicion and form queries that we should not have to deal with. The last ethical dilemma we discuss is that location-based services promote immoral acts. When separate entities can track where you are going and where you’ve been, this simply greatens the possibilities of immoral acts and resistance becomes more difficult. If we start taking advantage of these possibilities, then we begin to oppose our character-based ethics we all try to live by.

Introduction:

An important privacy-related legislation is the U.S. Privacy Act of 1974. This legislation “gives substance to the idea of fair information practices including openness and transparency,
for example, no secret record keeping, individual participation, collection and use limitations, reasonable security and accountability.” In addition, in 1999 the Wireless Communications and Public Safety Act, more commonly known as the E911 Act classified wireless location information as Customer Proprietary Network Information (CPNI) along with “time, date, duration of a call, and the number dialed.” At the same time, Congress amended Section 222 to explicitly require, express prior authorization. The rules of Section 222 requires “individuals be given notice of the collection of information and its intended uses; businesses use information solely for the consumer initiated transaction; businesses gain individual’s permission (an “opt-in” standard) prior to using personal information for secondary purposes such as marketing; businesses gain individuals permission prior to disclosing personal information to third parties; and finally that businesses must provide consumers access to the information stored about them.”

Currently there are two types of classifications for location-aware services: location-tracking and position-aware. Location-tracking services rely on second parties to collect and retain information sent by the location devices, most often GPS or GSM service-based. Position-aware services are fundamentally based on the device itself knowing its location. Personal privacy is being compromised by the intrusiveness of location-based services and its exposure of personal information to third parties.

According to Dr. Alan F. Westin, Professor of Public Law and Government Emeritus at Columbia University, “Privacy is the claim of individuals, groups, and institutions to determine for themselves, when, how, and to what extent information about them is communicated to others.” It is clear that as long as technology continues to create and advance communication, there will be no such thing as complete privacy, companies that provide technological services require personal information for convenience and billing purposes. However, it is difficult to claim that because of the technological advances, our society of consumers should have less privacy regarding the information pertaining to their own persons. The pace at which LBS technology is advancing is rapid and it is increasingly adhering to everyday life. Location-based services are at the point to which they can be used at any time, regardless of whether or not the user is aware. Simply by making a phone call, information is recorded with the potential of being accessed by anyone extending from corporations to the government and even to individuals.

The potential for misuse of this information is overwhelming. The government could deem that someone is spending what is considered to be “too much time” in the wrong part of town and suddenly this person is suspicious. This is the case, even though that may just be where you go grocery shopping. It is a very real possibility that a thief could use LBS to watch for when you leave your house and rob you while you are out. It is clear that, “because location information reveals, often in real-time, the whereabouts of the individual, the potential for privacy intrusion and other harms is more serious than with other types of personal information.” Personal privacy is becoming extremely vulnerable because of location based services and, “without the ability to control the collection of location information, consumers may lose the privacy safeguards currently afforded by other federal and state privacy laws.” The security of your information is limited and you have no control over the content or degree to which the data is shared. It is clear that while these services have very useful attributes, there is plenty of concern amongst the public for privacy protection.

Louise Barkuus and Anind Dey documented a case study they performed that shows individuals opinions on the subject. Barkuus and Dey gave sixteen participants four hypothetical
features for their phones. Two services were location-based and the other two were position-aware. Next they recorded their opinions on each service. The participants thought one location-tracking based service (being able to locate friends) and one position-aware service (private ringing profile) were the most useful, however the two location-tracking services were rated much more intrusive than the position-aware services. Their final results showed that consumers generally like location-based services as long as they are deemed useful. They also found that the location-tracking services cause more concern than the position-aware services do because, “the level of intrusiveness and concerns for privacy are much higher for location tracking than for position-aware services.”\(^5\) These results are shown in the following tables:

---

**E911:**

As previously stated, there are definitely some good uses for location-based services. The best use as of right now is the E911 service. This service is already applied to many mobile devices now and the basic idea is that in an emergency, the phone will alert paramedics of your location to get help as soon as possible. This is a great feature that does have proper mandates on it. It is assumed that this service is ethical and does not invade personal privacy, however the increasing technology of LBS continues to improve their other services, which provide plenty of concern over a variety of ethical frameworks.

**Support for Arguments Against LBS:**

Today the threat of the misuse of technological services is very real. Personal privacy is at risk with the free flow of information provided by the Internet and other networking programs. In 2006, independent electronic-security experts managed to use a technique known as pretexting to obtain the phone records of Hewlett-Packard board members and a number of journalists. Pretexting is the process in which ‘hackers’ fraudulently gain access to classified information. In this particular case, the use of a board member’s phone number and the last four digits of his or her social security number would allow any access to the records of calls made from the account in question. Incidents such as this legitimize concerns with the security of wireless services; this is to say the availability or difficulty to obtain personal information shared by wireless networks. Unfortunately for consumers, there is no specific federal protection against such acts of pretexting. As it stands there is no protection to prevent similar methods in order to obtain the records of your past and current location logs.\(^1\)

At any time ‘hackers’ such as these could obtain your history of locations. This information may include your home, your office, your mother’s house or even your children’s
daycare center. However, it is not just the threat of ‘hackers’ and malicious third parties to whom your information is made available, corporations have access as well.

Marketers are currently using LBS to promote products or establishments within a certain geographical radius. Cybermarketers have the capabilities to create location-based customized voicemail or text messages sent to a mobile device. As a person walks through a shopping mall, the mobile device that they carry with them can be contacted once it is in a certain range of a store, and sent a message notifying the user of a sale. At first glance, this use of LBS would seem nothing more than a minor nuisance; however, the location-based spam would become costly for certain phone plans as each message has a charge associated with it. While it is common practice for companies to buy and sell telephone and mailing lists, this may also become common for the trading of location traces. As previously stated, location data could be detrimental to your reputation or risk assessment if misinterpreted by a third party.

**Arguments Against LBS:**

The first ethical framework that location-based services contradict is that of utilitarian theory. It is in the utilitarian framework that one analyzes an ethical dilemma and bases a decision by determining which option provides the greatest good or the least harm for all who are affected. By making a decision one would hope to increase the good done and reduce the harm. Location-tracking and position-aware services do not ultimately provide more good than bad. It is reasonable to assume that if LBS continue to grow and become more common, that the usability will grow with it. It is the nature of technology to make devices easier and cheaper to use over time. As a result of that, those devices become more prevalent commodities for the population. Just looking at early cell phones shows how large and complicated they were; few people used them. However, as technology advanced, the phones became simple to use and conveniently smaller. Now they are so prevalent that some people have replaced their home phones with the cell phone. Technological features become standardized and they must in order for companies to stay competitive. With an easier usability of LBS it would make sense that more people would use the services and could apply them to every day life. Friends could easily locate each other. Parents could keep track of their children. With no restrictions on how this service is applied, it would create a society in which those with the desire and skill set could basically spy on anyone they wanted. It would create chaos. While the parents are monitoring their children to make sure they are safe, thieves could be monitoring those parents to see that they aren’t at home. This could also result in a society in which the government tracks anyone with a mobile device to make certain they aren’t doing anything suspicious.

The technology is currently so advanced that people do not need to make a call for most of these services to be activated. Imagine what it could be like in five years. People could not only be able to see where you’ve been and what you’ve been doing through your mp3 player, but they could see what songs you’ve been listening to the whole time as well. There would be no privacy at all. While it may be seem ideal to be able to tell that your best friend is just around the corner, it is not nearly as attractive when people with cruel intentions use that same technology. Although the features of LBS are enticing, when expanded to a broader scale, we can see that location-based services do not provide more potential for good than they do for harm.

Another framework that makes location-based services undesirable is the idea of duty-based ethics. As humans, we all have an obligation to not steal, hurt, or mistreat one another. The idea of LBS and the ways this information is being used can and will inevitably hurt us. It is undeniable that eventually this technology will be misused and individuals will suffer the backlashes. Every time an employer or a recruiter suspects or perceives that you are a part of an
“un-American” group or of a particular religion or sexual affiliation because of some tracking device, that individual will suffer unjust consequences. Because your monitored location shows perceptions of you in a certain way or perceptions that you are affiliated with certain people does not make that assumption correct, nor does it make the idea of knowing such information reliable. It is every human’s duty to not let such technology become the deciding factor for trust, loyalty and honesty. Every human deserves the right to control the content of the sensitive materials regarding their own person. The duty of every human to protect that right is too easily compromised by LBS and their access to the sensitive material. This brings about the idea of innocent until proven guilty, but LBS promotes the opposite of this; this technology promotes the idea that everyone is guilty under suspicion of being a certain way and/or of participating in a certain behavior. The idea of ethics under a rights approach is that the ethical action should be the one that best protects and respects the moral rights of those affected. The technology behind LBS does not protect nor respect human’s rights; in fact, it does the opposite by putting the actions of every human under scrutiny and ridicule most often without the opportunity to a defense.

The last ethical framework that opposes LBS is the theory of character-based ethics. This theory based on morals is contradicted by LBS. LBS do not provide a motive for being moral, but they do provide many opportunities to be immoral. The opportunities could be as simple as using any gained information to get what you ultimately want. Even worse, it could be used as blackmail in hopes to corner another and, in return, not reveal whatever compromising information you may have on them. More importantly, most people would be going against their virtues, which according to early philosophers like Plato and Aristotle, are needed to be a moral person. Using information gathered from services like LBS would have people ignoring their original training of good habits and character traits, which according to those early philosophers, is what we all need to live well.

Being virtuous implies living up to and acting to the highest possible potential of one’s being. Using location-tracking and position-aware services that LBS provide puts into question everyone’s whereabouts, intentions and actions and provides a more volatile country. Inevitably this volatility would form between anyone who is using LBS. It would cause issues between the government and its citizens, businesses and its employees, even between parents and children. There would be a huge division between those who are using the services to monitor people and those who are being monitored. This service could very well pose as helping locate or watching potential security risks and then very easily move to watching everyone and anyone by whomever within the public. This service will have people relying on a piece of technology to never lie to them, to give enough information that makes assumptions and interprets them as suspicious, and it would be looked at as true. LBS will take away the human factor from its user and place each consumer in a position that puts their every movement and action under watch by not only businesses and the government but their friends and loved ones as well.

**Conclusion:**

Like most technological advances, there are harmful consequences to those developments that began as ideas of good intent. Location-based services can be useful for directions, nearby facilities, and as tracking tools for emergency situations. Location-tracking and position-aware devices are emerging into the mass production of many mobile devices. As they become more common, the potential for unethical operations begins to surface. From a utilitarian standpoint, these services would enable an entire population of spies and stalkers through its invasive technology. This newly found power would threaten your safety as a person with an enabled
mobile device and those associated with you. Not only would you and your contacts’ physical safety be in danger, but your reputation would also be at risk to the interpretation of your location information. Your attendance at a civil rights rally, a stop at an abortion clinic, a trip to a gun shop, or even the frequent pattern in your fast food selections; all will be up to interpretation. As a duty-based argument, a person’s safety should be honored and protected by all. Since LBS are analyzed and assessed through interpretation alone, data would be manipulated and spun so that anyone’s chronological activities could be misinterpreted as being suspicious in nature. This suspicion and documented information would have considerable leverage over your character and virtue as a moral individual. No longer is the safety of your life and reputation being honored or protected but instead being manipulated and misrepresented in resulting detriment.

This idea of an entire population being threatened by a technological advancement is not abstract. The process of sharing information has become easier through the prevalence of wireless networks and services. With the right knowledge of the systems, anonymous third parties can obtain and gain access to your records through fraudulent tactics. The data may also be intercepted through the wireless signal from which it is shared. The cybermarketers that use these methods to advertise and promote through LBS are indications of the vulnerabilities of the information stored on mobile devices. Location-based services would become another method of sharing personal information through a system of networks. Although the services are helpful in theory, the harm caused by the ease of manipulation of your information for personal benefit concludes that the mass implementation of LBS is unethical.

Work Cited


Markkula Center for Applied Ethics. “A Framework for Thinking Ethically”. Pg. 2
<http://www.scu.edu/ethics/practicing/decision/framework.html>

Federal Trade Commission. Section 5 of the FTC Act. “Unfairness and Deception”.
<http://www.ftc.gov/privacy/privacyinitiatives/promises.html>


Markkula Center for Applied Ethics. “A Framework for Thinking Ethically”. Pg. 2
<http://www.scu.edu/ethics/practicing/decision/framework.html>