Privacy and Ethical Issues in Location-Based Tracking Systems

Jessa Liying Wang and Michael C. Loui
University of Illinois at Urbana-Champaign
lwang41@illinois.edu, loui@illinois.edu

Abstract

Location-based tracking systems (LTSs) use a variety of technologies to record the locations of objects. An LTS can increase the risks to the privacy and security of individuals. Previous studies have failed to distinguish between losses and violations of privacy when the locations of individuals are recorded by an LTS. We argue that individual privacy is threatened not by the collection of public location information but by the centralization of aggregated information, and by the combination of location information with other personal information. Further, informed consent should be required when the collection of information might cause a violation of privacy.

1. Introduction

At a boutique in Singapore, Chris purchased a fashionable new leather jacket at a low price. Walking out of the boutique, Chris was completely unaware that around the corner, a stranger with an RFID scanner had picked up the signal from the RFID tag embedded within the threads of Chris's jacket. While Chris fished a smartphone out from a jacket pocket and tried to locate a nearby restaurant for lunch, a base station picked up the GSM signal from the phone and pinpointed its location to a telecommunications operator who was tracking customers whose cell phone fees were overdue. The operator sent a text message to Chris's smartphone with a bill reminder, which included a list of authorized payment centres in the vicinity. Chris used the smartphone's GPS feature to search for directions to the nearest payment centre and to a restaurant with decent Chinese food. Based on Chris's personal profile, the GPS server sent a couple of digital food coupons to Chris's phone, to use at the Chinese restaurant.

This story illustrates some of the benefits and risks of location tracking technologies. RFID tags enabled the manufacturer, distributor, and retailer of the leather jacket to improve their efficiency in stock management and to save labor costs. The GPS and GSM location services saved Chris substantial time in finding a payment centre and a restaurant. Despite these benefits in cost and convenience, Chris was unaware of the security risks, specially the irreversible loss of privacy when Chris's personal information was shared.

Previous studies of location-based tracking systems (LTS) have briefly mentioned their ethical implications, but have ignored the problem of user awareness. In this paper, we distinguish carefully between losses and violations of privacy in LTSs, because even in public places, individuals deserve some privacy. We argue that individual privacy is threatened not by the collection of personal information alone but from the aggregation and centralization of personal information. Finally, in the absence of applicable laws, we propose conditions under which technical standards should require the explicit consent of individuals when their locations are tracked.

2. Location tracking technologies and their uses

2.1. Global positioning systems

A Global Positioning System (GPS) uses a constellation of GPS satellites that orbit the earth. These satellites broadcast messages on radio frequencies that consist of the time of the message and orbital information. A GPS receiver measures the transit times of messages from four satellites to determine its distance from each satellite, and thereby calculate its location.

In the United States, law enforcement officials use GPS technology to track criminal suspects and parolees without their awareness. For example, they may attach to the individual's car a device such as Trackstick,™ which is a GPS data logger integrated with GoogleEarth [1]. Law enforcement officials argue that GPS devices fall outside the scope of laws regulating wiretaps and similar forms of electronic surveillance because they do not record conversations [2].

Some states have considered requiring GPS devices on all motor vehicles, to track the distances that they travel. Then states could collect taxes from motorists, in proportion to their mileage, to pay for the construction and maintenance of highways [3]. These vehicle mileage taxes would replace gasoline taxes, whose revenues will decline as the number of electric and hybrid-powered cars increases.

GPSs are used by businesses, such as package delivery services, to track employees who travel to multiple

locations during each work day. Some employers use the location history of employees to infer their intentions or to construct social networking relationships [4]. Because GPS devices are often integrated into cell phones, individuals may be unaware that their locations are recorded whenever their cell phones are turned on.

2.2. Radio frequency identification tags

A radio frequency identification (RFID) tag consists of a microchip and an antenna. The typical tag ranges in size from a postage stamp to a pager. Each tag stores a unique identification number. An active RFID tag, which has its own power source, can transmit identification information up to a mile away. A passive RFID tag, which is activated by an external source of power, can transmit information up to 20 or 30 feet [5].

In Singapore, RFIDs are embedded in smartcards (EZ-Link cards), which are used for contactless payment on public trains and buses. Because each EZ-Link card is associated with the individual's national identity number, public transportation providers can track the individual travel histories of their customers. Each travel transaction is stored on a central server. When the EZ-Link card is presented to a card reader at a train station, the customer's last fifty transactions are displayed [6].

Since January 1, 2007, the U.S. State Department has issued passports with embedded always-on RFIDs. Individuals who try to disable the RFID chips are subject to a prison sentence of up to twenty-five years [7].

In the commercial sector, RFID tags on products are used to manage inventories and supply chains. For example, clothing articles marketed by Calvin Klein, Abercrombie & Fitch, and Champion contain labels with concealed RFID tags. These tags can be read by RFID scanners at the exits of retail stores to verify purchases and deter theft. Some companies have used RFID tags to monitor individual customers too. In a Wal-Mart store in the United States, as customers picked up RFID-tagged Gillette razor packages, close-up photographs of their faces were taken. In a Wal-Mart store in Oklahoma, customers who sampled Procter & Gamble Lipfinity lipstick were monitored with a webcam [8].

2.3. Global system for mobile communication

The Global System for Mobile Communication (GSM) provides personalized services to cell phone subscribers based on their current locations. A GSM uses several methods to find the location of a subscriber. These methods use the time taken by signals to travel between the subscriber's handset and the cellular network base stations.

GSM is used in intelligent transportation systems to monitor traffic conditions. GSM signals emitted by cell phones in vehicles can automatically report their positions, travel time, traffic incidents, and road surface problems [9].

3. Privacy and security risks

At this time, no laws or regulations explicitly limit the applications of LTSs [2]. The proliferation of LTSs has increased risks to the privacy and security of individuals.

An RFID reader can gather the identification numbers from the articles of clothing carried or worn by an individual customer. These numbers can be aggregated to create a composite portrait of that customer's shopping history—especially when combined with personal information about the customer stored in a central database. Although the RFID industry has assured lawmakers and consumer groups that RFID tags are intended primarily for inventory tracking, because RFID tags can remain operational after purchases, they can threaten individual privacy.

Even more insidious are risks to individual security from identity theft. At an EZ-Link reader, and at a passport reader, an intruder with an RFID scanner could steal the identification number of an individual, and then subsequently use that number to pose as that individual.

4. Ethical implications of location-based tracking service

Glasser et al. [10] compared RFID tracking to credit cards. In both cases, individuals present unique identification numbers in an authentication process, as evidence that they are who they claim to be. According to Glasser et al., "RFID [*sic*] does not violate privacy any more than credit card and bar code use, unless intruders have access to readers and the associated databases." But RFIDs and credit cards differ because owners of credit cards know that their purchases are recorded—they receive lists of their purchases with their monthly statements. A customer can choose between using a credit card and using cash to avoid tracking.

Other previous studies [11], [12], [13], [14], [15] have described how LTSs threaten the privacy of individuals. For example, LTSs collect location information silently, without the permission or even the awareness of individuals. Although it appears that individuals have lost control over this information, and hence have lost their privacy, we note that technological devices perform many functions without seeking explicit permission and without notifying affected people. Automatic transmissions in cars change gears, and thermostats in houses turn on air conditioners, without the knowledge of their occupants. So the failure of LTSs to inform individuals is not necessarily unethical.

Previous studies have also neglected to distinguish between the **losses** and the **violations** of privacy caused by LTSs. This distinction is ethically significant [16].

To understand the distinction between a loss and a violation of privacy, suppose someone with binoculars observes you as you walk from one end of a city park to the other. The observer tracks your location just like an LTS, and you have experienced a **loss** of individual privacy. In this situation, however, you are walking in a public place, and you have no normative right to privacy from observation. We are not claiming that you never have privacy rights in a public place, however. When you are shopping in public, you have a right to expect that bystanders will not examine your shopping cart to record your purchases [17].

Now suppose several different observers notice when you cross the city park, which bus you take, where you leave the bus, and which building you then enter. If these observers combine their information, you would feel that your privacy has been **violated**.

Lin and Loui [18] emphasized that it is this **centralization** of aggregated information that violates your moral right to privacy. According to Rachels [19], privacy is valuable because it provides a context for individuals to create and maintain a variety of human relationships. The personal information that you share with a friend or a spouse differs from the information that you share with a business colleague. Lin and Loui explain that the centralization of personal information is unethical because it eliminates the context that privacy provides.

Several scholars have argued that when the collection of personal information might cause a violation of privacy, informed consent seems necessary [18], [20]. For example, Bhaduri [21] proposed to give customers of LTS systems the option of selecting the types of GPS location data that may be harvested. If the customer selects "pull services," the clients of the GPS service may not be told the customer's location, or they may be provided that location only when the customer makes a specific request that requires the location. If the customer selects "push services," the clients may advertise and offer discount services. Hedefine [22] proposed a "Do Not Link" registry on the Web, similar to the national "Do Not Call" list for telemarketers. When an individual registers on this Web site, businesses and governments would be forbidden from linking the individual's identity to products that contain RFID tags without the individual's explicit permission.

5. Conclusion

Location-based tracking systems (LTSs) are increasingly used by businesses to provide new services to customers. LTSs are also deployed by government entities to track potential criminals, and thereby to improve the security of communities. LTSs cause losses of individual privacy that are not necessarily violations of privacy. We have argued that LTSs threaten our individual privacy not because they collect personal information about our locations, but because they aggregate that information. In particular, when aggregated location information is combined with personal identifiers, the result is a potential violation of individual privacy. In these cases, informed consent ought to be necessary to balance the privacy rights of individuals against the freedom rights of businesses and the security rights of communities.

6. Acknowledgements

This work was supported by the National Science Foundation under Grants ERC-0628814 and IIS-0832843. The views, opinions, and conclusions of this paper are not necessarily those of the University of Illinois or the National Science Foundation.

7. References

[1] "GPS data logger widely used by law enforcement," UsaCops.com, Oct. 3, 2003. [Online]. Available: http://www.usacops.com. [Accessed: Oct. 3, 2008].

[2] E.M. Dowdell. "You are here! Mapping the boundaries of the Fourth Amendment with GPS technology," *Rutgers Computer and Technology Law Journal*, vol. 32, no. 1, pp. 109-139, 2005.

[3] J. Lowry. "Mileage tax considered by Obama transportation secretary LaHood," huffingtonpost.com, Feb. 20, 2009. [Online]. Available: http://www.huffingtonpost.com/2009/02/20/mileage-tax-considered-by_n_168506.html. [Accessed: Feb. 28, 2009].

[4] M. Wigan and R. Clarke. "Social impacts of transport surveillance," *Prometheus*, vol. 24, no. 4, pp. 389-403, Dec. 2006, quoted in M. U. Iqbal and S. Lim. "Privacy implications of automated GPS tracking and profiling," *The Second Workshop on the Social Implications of National Security: From Dataveillance to Überveillance and the Realpolitik of the Transparent Society,* pp. 225, 2007.

[5] "How radio frequency identification tags will help retailers, from supply chains to store shelves," *MIT Technology Review*, March 2004 [Online], Available: http://www.technologyreview.com/computing/13509/ [Accessed: Oct. 2, 2008].

[6] X. Yang, "Advanced public transport system in Singapore," *Proceedings, 6th International IEEE Conference on Intelligent Transportation Systems*, 2003, vol. 2, pp. 1660-1663.

[7] "How To: Disable Your Passport's RFID Chip," *Wired*, Jan. 2007 [Online], Available: http://www.wired.com/wired/archive/15.01/start.html?pg=9 [Accessed: Sept 2008]

[8] K. Albrecht and L. McIntyre. CASPIAN Consumer Privacy, "RFID: Big Brother's barcode," *ALEC Policy Forum*, vol. 6, no. 3, pp. 49-54, Winter 2004.

[9] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Enhancing security and privacy in traffic-monitoring systems," *IEEE Pervasive Computing*, vol. 5, no. 4, pp. 38-46, Oct.-Dec. 2006.

[10] D.J. Glasser, K.W. Goodman, and N.G. Einspruch, "Chips, tags and scanners: ethical challenges for radio frequency identification," *Ethics and Information Technology*, vol. 9, no. 2, pp. 101-109, July 2007.

[11] V. Lockton and R.S. Rosenberg, "RFID: the next serious threat to privacy," *Ethics and Information Technology*, vol. 7, no. 4, pp. 221-231, Dec. 2005.

[12] M.G. Michael, S.J. Fusco, and K. Michael. "A research note on ethics in the emerging age of uberveillance (überveillance)," *Computer Communications*, vol. 31, no. 6, pp. 1192-1199, 2008.

[13] L. Perusco and K. Michael, "Control, trust, privacy, and security: evaluating location-based services" *IEEE Technology and Society Magazine*, vol. 26. no. 1, pp. 4-16, Spring 2007.

[14] A.R. Peslak, "An ethical exploration of privacy and radio frequency identification," *Journal of Business Ethics*, vol. 59, no. 4, pp. 327-345, July 2005.

[15] D.M. Wasieleski and M. Gal-Or, "An enquiry into the ethical efficacy of the use of radio frequency identification technology," *Ethics and Information Technology*, vol. 10, no. 1, pp. 27-40, Mar. 2008.

[16] J.H. Moor, "The ethics of privacy protection," *Library Trends*, vol. 39, no. 1-2, pp. 69-82, Summer/Fall 1990.

[17] H. Nissenbaum. "Toward an approach to privacy in public: challenges of information technology," *Ethics and Behavior*, vol. 7, no. 3, pp. 207-219, 1997.

[18] D. Lin and M.C. Loui, "Taking the byte out of cookies: privacy, consent, and the Web," *Computers and Society*, vol. 28, no. 2, pp. 39-51, June 1998.

[19] J. Rachels, "Why privacy is important," in D. G. Johnson and H. Nissenbaum, eds., *Computers, Ethics & Social Values*, Upper Saddle River, N.J.: Prentice Hall, 1995, pp. 351-357.

[20] J. Borenstein, "Privacy: a non-existent entity," *IEEE Technology and Society Magazine*, vol. 27, no. 4, pp. 20-26, Winter 2008.

[21] A. Bhaduri, *User Controlled Privacy Protection in Location-Based Services*, Master's Thesis, University of Maine, 2003.

[22] E. Hedefine, *Personal Privacy Protection within Pervasive RFID Environments*, Master's Thesis, University of Maine, 2006.