2001

# Wireless Applications: Influences and Risks of Location Identification Technologies

Raj Gururajan
*Murdoch University*, r.gururajan@murdoch.edu.au

# Wireless Applications: Influences and Risks of Location Identification Technologies

Raj Gururajan

School of Information Technology
Murdoch University, Murdoch, Australia
r.gururajan@murdoch.edu.au

**Abstract**

*With the advent of Wireless Application Protocols (WAP), location technologies have gained sudden importance. These location technologies combined with wireless devices (or commonly known as mobile devices) assist organisations to locate and precisely identify individuals. While the technology is a boon to instant marketing, certain implications associated with security and privacy has been questioned in recent weeks. This paper provides a discussion on the type of location technologies used in a wireless application domain, their influences in terms of identifying individuals and associated applications, and the implications in the uptake of electronic commerce.*

**Keywords**

Mobile Commerce, Privacy, Security

## INTRODUCTION

In the past 5 years a number of commercial applications have developed to locate and track inanimate objects including vehicles, equipment, cargo containers and packages (Schiller, 2000). The motivation for such development includes efficiency in production and logistics, and the security of assets. In recent months, software development projects have been contracted by Australian Government to some educational institutions to track endangered species of animals in order to identify their location and movement, to study their habits and to protect them. These location identification technologies involve specifically attaching an electronic tag to these objects or animals, and when these objects cross a predefined location, read the electronic tag, and identify the object.

When the concept is extended to humans, it is possible to identify individuals based on certain specific parameters such as a financial transaction. For instance, cases have been reported in the literature how some of the enforcing authorities have identified locations of individuals based on a visa card transaction(Anonymous, 2000; Budhwani, 2000). In countries like Australia, taxis and buses are located for monitoring purposes as well as security and safety purposes.

While these location identification technologies identify only objects and not humans, the acceptance of these technologies is not controversial. However, with the wireless applications, it is possible to identify and to extent precisely identify individual who use mobile devices such as a mobile telephone. When this identification is facilitated, the privacy of individuals is penetrated leading to concern (Warrington, Abgrab, & Caldwell, 2000). Further, it is identified that this privacy may further lead into potential security problems. So, while the influence of these technologies on electronic commerce technologies is significant, the implications may lead into security and privacy breaches. The following paragraphs provide a discussion on these issues.

## TERMINOLOGY

An entity's location usually describes its whereabouts or certain reference points (Schiller, 2000). The location can be ascertained by varying degrees of precision. The measures of location may be available with varying degrees of timeliness. Tracking refers to the plotting of a trail or a sequence of locations, within a space that is followed by an entity over a period of time (Dornan, 2001). The space is generally known as physical space or geographical space. A real-time trace refers to identification of an object or person at any particular point in time, with a degree of precision (Smith & Andrews, 2001).

The above terms provide an indication that by tracking a person at varying time intervals, it is possible to observe his/her behaviour. When multiple persons are tracked, then it is possible to observe group behaviour. Therefore, location identification technologies provide the power to make decisions about the entity subjects and hence to exercise certain amount of control over these subjects.

## INFLUENCES OF LOCATION IDENTIFICATION TECHNOLOGIES

In earlier days, the location identification technologies were usually used in homes and community areas. Examples of these are meter boxes for electricity reading and post boxes. Telephone books also come under this category. However, in recent years, location identification devices are used to capture movement of individuals and transaction data (Hulme, 2000). For instance, for security purposes, movement of police people are identified using some form of location identifier such as a wireless phone. Credit cards and debit cards also identify location of occurrence of financial transactions.

However, with the advent of 'smart card' technologies, the identification techniques have improved in its usage. These smart cards can identify a person based on the characteristics entered in the 'chip' and in conjunction with a location, may allow entry to the person who possesses the card. Certain security measures are usually incorporated in these smart cards to avoid any unauthorised use (Deise, Nowikow, King, & Wright, 2000).

Telecommunication advancement has assisted in locating certain characteristics of identification such as telephone number. For instance, when a person rings up, it is possible to identify the caller based on the number displayed on the telephone panel (provided one is available) and then respond to the call.

The recent advent of radio frequency based systems can identify individuals based on the devices they are carrying (Anonymous, 2000). For instance the Global Positioning System (GPS) identifies positional reference points using satellite signals. Closed Circuit TV (CCTV) is also another location identification system, which merely monitors the movement of individuals (McConnel, 2000). None of the above systems intrudes in the privacy and security of individuals.

However, the recent mobile devices such as mobile computers and telephones can identify individuals and further become an intrusion to their privacy and security (this is discussed in the next section). Using infrared technologies, it is possible to transfer information about location of buses and the number of people in the bus etc in order to optimise transport logistics.

## RISKS

In the area of electronic commerce, these location identification technology leads to four major areas of concern (McCullagh, Little, & Caelli, 1998): (i) Individual dangers; (ii) Social dangers; (iii) Organisation danger; and (iv) Privacy invasion. While there are other dangers involved, these four appear to be impacting the uptake of electronic commerce in a large scale.

Individual Dangers

In recent months, it has been mentioned in the media that is possible to locate an individual using a mobile device through a mobile telephone number of IP address in a wireless mode (Hayes, 2001). When such identification is successful, it is possible to approach that individual and this may lead to potential security problems. Even if the individual can't be identified, it is possible to steal data from the mobile device such as a mobile computer leading to potential dangers. Further, people entering a WAP zone can be targeted with notices containing viruses, effectively paralysing various functions of their computer. Even if viruses are not passed, it is possible to send unwanted information and simply drain the battery. When individual communicate using mobile devices, then it is possible to steal data in a WAP zone (Dornan, 2001). These are some of the known dangers and risks.

In terms of other dangers, it is possible to discover an individual's behaviour pattern using the location identification technologies and governments can use this in order to generate suspicion. Organisations can classify individuals in order to manipulate consumer behaviour. Further, once identified, individuals can be blackmailed. In addition, these location identification technologies can be used as 'evidence' in criminal cases.

Social Dangers

Social dangers assume greater significance because when identified, individuals involved in the act are subject to being exposed and assumed to have performed the act. The interpretation may be right or wrong but the very nature that a person was identified to have associated with an act rises public perception and hence leads to social action on that individual. For instance, a person was associated with a murder case in NewZeland in June 2001, and his identity was published in a local Internet site, leading to the accusation of charges on the person by public. The person was only in the vicinity of the murder and in way associated with the murder and the damage caused was irreparable. While this example was pertinent to the Internet media, in wireless application, this situation is not far away.

Organisational Danger

Organisations may encounter problems associated with wireless data. For instance, if mobile devices lack proper authentication procedures, then it is possible for an intruder to get access to the mobile devices and make use of the service facilities (Deise et al., 2000). Such abuses may put organisational data in danger. Further, it is possible to send wrong data to organisations using the mobile communication technologies, negatively influencing the decision making process.

Another possible situation is that a person having illegal access to an organisation's mobile device can access the customers and try to send them wrong information. Such an act will create pad publicity for an organisation and in some cases will end up in legal battle. Organisations have to protect themselves from these risks in a mobile e-commerce environment.

Privacy Invasion

In an e-commerce environment, the location identification devices appear to generate concern in privacy issues. Recent reports (Green, 2000) indicate that consumers are worried about their privacy and potential intrusion to privacy when mobile devices are used. In certain financial transactions, consumers would like to be anonymous. The anonymity can be revealed in a mobile commerce environment with the assistance of location identification devices. In areas such as health, revealing patient details may violate privacy regulations in certain countries. Governments are in the process of modifying their privacy laws but more work needed to tighten various loopholes caused by modern technologies.

## CONCLUSION

While the future of wireless application is bright, various issues such as privacy need to be sorted out before consumers accept the technology. Combined with location identification technology, wireless application open out some interesting applications. There are some recent changes to privacy laws associated with information technology. However, organisations appear to have difficulty in implementing them. The four risk areas mentioned in this paper is further being considered for a survey in Western Australia with specific focus paid to regulatory framework. The subjects of the survey will comprise of industries, consumers and government agencies in order to determine the awareness of privacy and security issues among these consumers in a wireless application domain.

## REFERENCES

Anonymous. (2000). Wireless technology reaches behind the firewall. *Informationweek.com*(June), 30.

Budhwani, K. (2000). Becoming part of e-Business. *CMA Magazine*, 24-27.

Deise, M. V., Nowikow, C., King, P., & Wright, A. (2000). *Executive's Guide to e-Business: From Tactics to Strategy*. New York: John Wiley & Sons, Inc.

Dornan, R. (2001). *The essential guide to wireless communication applications*. Upper Saddle River, NJ: Prentice Hall PTR.

Green, P. (2000, 4 June). Eastern Europe's Foary into M-Commerce. *The New York Times*, pp. 3.8.

Hayes, S. (2001, 27 February 2001). Indian Giant Wants Service Satff. *The Australian*, pp. 38.

Hulme, G. (2000). Services Seeks to Bring e-Business to Small Businesses. *Informationweek.com, August 2000*, 21.

McConnel, B. (2000). Kennard pushes cable DTV. *Broadcasting & Cable*(February), 37.

McCullagh, A., Little, P., & Caelli, W. (1998). Electronic Signatures: Understand the past to develop the future. *University of NSW Law Journal, 21*(2), 1-13.

Schiller, J. (2000). *Mobile Communications*. New York: Addison-Wesley.

Smith, D., & Andrews, W. (2001). *Exploring Instant Messaging*.: Gartner Research and Advisory Services.

Warrington, T. B., Abgrab, N. J., & Caldwell, H. M. (2000). Building Trust to Develop Competitive Advantages in e-Business Relationships. *CR, 10*(2), 160-168.

## COPYRIGHT