PRIVACY CHALLENGES FOR LOCATION AWARE TECHNOLOGIES

Carl Adams and Vasilios Katos
School of Computing, University of Portsmouth, PO1 3AE, UK

Abstract: Location aware capabilities can supply context and location sensitive information and support enabling users to be contactable and locatable within a wider mobile environment. These location awareness attributes can also be used to monitor user activities and movement through space and time. This paper explores location aware technologies and the resulting changing privacy and security landscapes for such mobile systems. The paper argues that the real challenge of meeting privacy obligations will be how to limit the joining-up or collaboration between the different monitoring technologies. However, this joining up capability is the very nature of information systems.

Keywords: Mobile Information Systems, Privacy, Security, Location Aware Technology

1. INTRODUCTION

A trend facing business and technology arenas is the move towards ubiquitous wireless technologies, which is having considerable strategic impact, fundamentally changing business models and processes (Barnes 2003,p2). Mobile information systems have location aware capabilities, providing context and location sensitive support. Some location awareness is also needed to provide access to the corporate infrastructure and systems, enabling users to be contactable and locatable within a wider environment. This paper explores location aware attributes and the implications of combining data from different sources. In addition the paper examines how the use and functionality of technology changes over time as users' needs change, using CCTV technologies as an example. Development of information systems with mobile capabilities has to recognise these location

aware attributes and the evolving nature of technology. There are clearly wider implications for business, and for developing mobile systems.

2. MONITORING FUNCTIONS OF TECHNOLOGY

Increasingly technology is used to monitor peoples' activity. The majority of the monitoring activities have been introduced for sound reasons such as ensuring the safety of pedestrians or protecting shoppers against fraud. However, monitoring activities raises privacy issues. Increasing monitoring activity has been the result of changes in business, technology and society. This has been most evident with CCTV. The UK is a 'good' example of this trend, as Privacy International (1995) identifies "[there has been an] extraordinary growth of the electronic visual surveillance industry ... In recent years, the use of Closed Circuit Television (CCTV) in the UK has grown to unprecedented levels". The number of CCTVs in the UK has grown dramatically since the mid 1990's, one estimate puts the number close to 4M (Lott 2005, p39). There are more CCTVs than the number of people able to sensibly monitor them. This clearly points towards automation and digitising of CCTV images. An example of wider use of such CCTV technologies is the introduction of congestion charging around London. This CCTV monitoring activity raises several privacy protection issues, as Spy.org (2005) identify: "We are not so much concerned with the actual congestion charge itself, but rather with the Privacy implications of the particular way in which this scheme has been implemented. ... The scheme relies on about 700 CCTV cameras covering around 203 entrances/exits to the 21 square kilometre central zone. Each lane of traffic either entering or leaving the boundary of the zone is covered by a [camera] linked to a Automatic Number Plate Recognition system".

The technology developed for congestion charging is now being used for other purposes. As The Register (2003) identifies, initially Ken Livingstone claimed that the system would only be used for congestion charging. However, only a short time after being introduced Ken indicated that the system can be used for other functions with cameras able to view drivers' faces, be controlled remotely and having variable angle and zoom facilities. In addition, the system would be used (when needed) to assist law enforcement activity.

Technologies evolve in how they are used: This concept is not new to most developers who have to contend with changing and evolving requirements. So a CCTV camera can be installed in a shopping space initially under the guise of addressing security issues, but evolves into a store management tool monitoring customer flows and purchase patterns.

initially under the guise of addressing security issues, but evolves into a store management tool monitoring customer flows and purchase patterns.

3. SECURITY AS THE MAIN DRIVER FOR MONITORING ACTIVITY

There are several drivers for increasing monitoring activity, not least because of an increased focus on security. Societal changes to be more security conscious has been recognised internationally in the OECD guidelines on promoting a global 'Culture of Security' (OECD 2003). The OECD's guidelines respond to the ever-changing nature of security and the wider environment, recognising the different roles and responsibilities for each 'participant' including Governments, businesses and society. The implications for owners and operators of information systems and networks are explicit in that they are expected to address the principles of risk assessment, and security design and implementation (ibid, p6). These changes in security focus, of course, have been influenced by events and changes in society, such as the 9/11 terrorist attacks in the US. In this global 'culture of security' Governments and corporations are expected to address security with appropriate policies and action, usually resulting in increasing collection and monitoring of information about employees and customers.

3.1 Data Protection and Privacy Issues

The increasing information collecting and storage capabilities of ICT have also resulted in increasing concerns over privacy issues. In the 1980's the OECD also developed a set of guidelines governing the protection of privacy (OECD 1980, p8). The guidelines identify a need for balance between privacy and economic needs to use, store and transmit such personal data to conduct transactions and support commerce. The guidelines identify basic principles for applying privacy protection laws, key of which is ensuring individuals have the opportunity of informed consent in the use of data about them. Governments and businesses have to achieve a somewhat difficult balance between meeting their security obligations on one-hand and privacy obligations on the other.

3.2 Implications of Mobile Location Aware Technologies

The potential for monitoring is likely to increase with the trends toward more mobile location aware technologies. Raina and Harsh (2002) describe

boundaries. This expansion of corporate space will also have a direct impact on privacy as information is transmitted over this wireless corporate space: "As a corporation's corporate space expands it may also overlap with other corporation's corporate space. The overlapping may result in and clashing of corporate spaces, or development of multi corporate wireless spaces where more than one business is operating and sharing mobile information" (Adams and Katos 2005). This expanded corporate or multi-corporate spaces may also encroach on individuals' personal space, or personal trust space (Adams et al 2003).

From a security perspective wireless technologies are inherently less secure opening the system up to attacks from outside the corporation's premises and providing an increase in potential security weak points (Panko 2004;Ciampa 2004, p22). Wireless security can be improved to reach (something equivalent to) the wired world but as Ciampa (2004, p23) identifies extra technologies and processes will be required. Increasingly wireless involves not just one mobile technology but an array of competing devices and infrastructure each with their own security (and privacy) issues.

From privacy perspective wireless technologies also raise more concerns as location information is embedded in the protocols or within system attributes. Many of the wireless devices are personal devices (e.g. PDAs, Bluetooth phones) attached to individuals and so likely contain personal information. They will also be locatable within an organisation space by association with their access points and interaction with other devices. It may even be possible to monitor movement of such devices, and their users, throughout the corporate space. The same monitoring capabilities are possible outside the corporate space. For instance, since 1996 wireless carriers in the US have been required to incorporate wireless phone locators in their networks for 'safety' reasons (WLIA 2001b) under the E911 (Enhance 9.1.1. the emergency services telephone number in the US) mandate as part of the Telecommunications Act of 1996. Similar early location based developments took place in Japan and Europe (ibid). Most wireless telecommunications infrastructures incorporate location information about users, embedded in operating protocols. With 3G technologies and always-on capabilities, such location information will become more accurate, pervasive and intrusive.

The importance of privacy and anonymity with location aware technologies has been recognised by the Wireless Location Industry Association (WLIA): "Without question, the single most important issue confronting the new industry of wireless signal location technology and applications is the issue of personal privacy. As with any other issue, there are two sides to this issue. This does not mean that there are two sides as in "for" or "against" privacy, nor two sides as in "for" or "against" wireless

Association (WLIA): "Without question, the single most important issue confronting the new industry of wireless signal location technology and applications is the issue of personal privacy. As with any other issue, there are two sides to this issue. This does not mean that there are two sides as in "for" or "against" privacy, nor two sides as in "for" or "against" wireless signal location. Reasonable people will look for solutions that will maintain both the value of protecting individual privacy and the value of achieving the benefits of new wireless location technologies. The issue is how to strike the right balance between these values." (WLIA 2001a)

The WLIA have been involved in developing a set of self regulation policies for operators involved in location monitoring activity, these include the Fair Location Information Practice (FLIP) (Barnes 2003, p144; WLIA 2001a), key of which is also ensuring individuals have the opportunity of informed consent in the use of location data about themselves. However, there are practical challenges in applying the FLIP guidelines. For instance, most of the data collection activity is likely to be automatic. Even if some informed consent activity is possible, it is unlikely to be fully exercised since much of the data will to be collected and stored under security and monitoring obligations: Telecommunication operators and providers have to maintain logs of customer call activity, including location information (Adams and Katos 2005).

When more than one technology interoperates, the privacy space may shrink substantially. For example, a CRM related technology employed by a supermarket might use customer loyalty cards. The purpose of these cards is to collect valuable marketing information related to buying patterns; the customer willingly sacrifices a 'small amount' of privacy for a minuscule financial gain. However, even with customers without loyalty cards, hypothetically at least, companies are still able to populate their CRM database by combining transaction information with CCTV or with information broadcasted by any wireless personal devices a customer may have (bluetooth, RFIDS etc). This raises a more fundamental privacy challenge. The privacy landscapes are likely to change considerably once there is 'joining up' between monitoring technologies. Combining data from more than one source enables a richer set of data to be collected about individuals. All the monitored data can be stored electronically, possibly on the same computer systems. All the technology seems to be in place to bring together the different monitoring activity: Not only does a corporation have the capability to track what you buy but also how you entered the purchasing space and all the different activity in moving through that space right though to the purchasing. A psychologist analysing this information may be able to gleam considerably more information about individuals than the individuals may be aware of themselves!

4. EVOLVING USE OF LOCATION AWARE TECHNOLOGIES

As seen with the CCTV examples above, many of the CCTV monitoring technologies seem to fall outside the realms of data protection and privacy rules and controls. Equally there seems little to limit expanding the function and scope of using such technologies as well as collating and collaborating monitoring information from different sources.

The de facto approach in collection of location information seems to automatically imply consent to collecting and using information in what ever fashion the collectors' wish. The possibility of collaboration between location aware technologies is, at least in part, also likely to be automatic and location based services will require some joining up of information.

Take the example of the possible introduction of ID cards in the UK. ID cards are used in a variety of other countries, however, the proposed application in the UK will result in generating a vast repository of personal data on individuals in the UK, including biometrics (LSE 2005). The ID cards are likely to - at least in part - be in the form of contactless cards. During 2004 the proposed national ID card Bill had a rough ride through parliament and was not able to make it through the House of Lords before the call for new elections in the UK in 2005 (Privacy International 2005). However, very soon after the UK election in early May 2005, the continuing Labour Government reintroduced The Identity Cards Bill on the 25 May 2005 (UK Gov 2005). The UK Government seems serious about 'pushing through' a national biometric based ID card system. The same is true in the US where technological developments towards wireless ID cards is more advanced, along with the 'pushing through' of legislation. The US ID card bill in the US seems to have been passed through the senate on the back of an $83Bn funding bill for troops in Iraq and general homeland security (Privacy International 2005). In both the UK and US a rich set of personal and biometric information will be communicated over a wireless medium. Presumably there will be some demand to people to carry their electronic ID cards. A uniquely identifiable ID card with electronic communicating capabilities opens up a range of possible uses and more particularly for implementing authentication services. It could also be used for a range of other functions such as a driving licence, access to a toll both or corporate space or as the basis for facilitating electronic interactions such as e-voting. It is likely that many types of organisations will be interested in using such 'useful' devices and it would seem a natural progression to allow this. Commercial avenues may be an attractive proposition for governments that have spent the estimated tens of billion £'s taxpayers' money to develop the infrastructure (LSE 2005). Mobile information systems for such

organisations are likely to have access to very personal information, including the location and context relative information from any interaction with individuals.

With such an array of different wireless technologies ubiquitously available, including RFIDs, Bluetooth, WiFi, GPS and mobile phone technologies, then it seems a natural progression that corporations will be developing data contact and collection points with these. The use for these contact and collection points is also likely to evolve. The range and volume of personal data to be collected is growing and corporations' mobile information systems will be playing a part in managing this data and making sense of it. Making sense of vast amounts of information is what information systems do, and do remarkable well. Mobile information systems will also play a part in the natural evolution of the use of mobile technologies and seems a natural outcome of the 'making sense' process. The scenario described earlier of corporations being able to 'gleam considerably more information about individuals, more than the individuals may be aware of themselves' seems a natural outcome of the progression towards ubiquitous wireless systems.

5. CONCLUSION

This paper has contented that there has been an increase in the use of technology to monitor peoples' activity, and that there is increased potential for monitoring with the trend towards more mobile location aware technologies. Location aware capabilities offer potential benefits to customer and citizens, but equally they raise privacy issues. Individually the privacy issues are not insurmountable. However, as the use of such technologies unfold and develop, coupled with the capabilities of combining location information from different channels there are considerable impacts on privacy and anonymity. The trend towards location aware technologies seems inevitable. Also inevitable is an increase in the amount of location information collected, given that it is most automatic and part of the technology operation. The operation of the wireless technologies also makes joining up of monitoring activity more likely; indeed it will be a prerequisite for providing many location aware services.

This paper discussed the developing privacy landscapes, particularly with reference to mobile location aware technologies. The real challenge of protecting citizens' privacy will be how to limit the joining-up or collaboration between the different monitoring technologies, and this joining up capability and making sense of such joined up data is the very nature of information system. A real challenge for future mobile information systems

is how to protect privacy while managing a vast and growing set of location aware and, increasingly personal data.

References

Adams C., Avison D.E. and Millard P. (2003) Personal trust space in mobile commerce. Proceedings of ICECR-6, Dallas, Texas, Oct 23-26, 2003, p396–403.

Adams C. and Katos V. (2005) The ubiquitous mobile and location aware technologies time bomb. Cutter IT Journal, June 2005.

Barnes S. (2003) Mbusiness: The strategic implications of wireless communications. Elsevier Butterworth-Heinmann, London.

Brunk, B. (2003). A Framework for Understanding the Privacy Space. PhD Thesis, University of North Carolina.

Ciampa M. (2002) Guide to Wireless Communications. Thomson, Massachusetts.

Crimereduction.gov (2005) CCTV initiatives home page. A UK government, pro-CCTV web site. http://www.crimereduction.gov.uk/cctvminisite4.htm

HEW (1973). Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens (HEW Report). U.S. Department of Health, Education and Welfare.

Lott T. (2005) Every move you make. Times newspaper, Magazine, May 14th, p37-41.

LSE (2005) The Identity Projects: An assessment of the UK Identity Cards Bill and its implications. Version 1.09, June 27, 2005.London School of Economics.

Martin L. (2005) This chip makes sure you always buy you round. The Observer, 16th January 2005, p14.

OECD (1980) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD Publications, Paris. Also available from the web at www.oecd.org

OECD (2003) Implementation plan for the OECD guidelines for the security of information systems and networks: Towards a culture of security. Document DSTI/ICCP/REG(2003)/5/REV1, 02-July-2003, Organisation for Economic Co-operation and Development.

Olsen, S. (2000). Web browser offers incognito surfing. CNET News.com, http://news.com.com/ Web+browser+offers+incognito+surfing/2100-1017_3-247263.html

Panko R.R. (2004) Corporate Computer Network Security. Prentice-Hall, NJ.

Privacy International (2005) "UK ID Card Bill Dies" Available from http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-178984

Raina K. and Harsh A. (2002) mCommerce Security: A beginner's guide. McGraw-Hill/Osborne, California.

Schneier, B. (2000). Secrets & Lies. New York: John Wiley & Sons.

Spy.org (2005) London Congestion Charge CCTV privacy concerns. From http://www.spy.org.uk/cgi-bin/cclondon.pl

The Register (2003) "London charge zone is security cordon too, says mayor" from http://www.theregister.co.uk/2003/02/17/london_charge_zone_is_security/

UK Gov (2005) Identity Cards Bill. http://www.publications.parliament.uk/pa/cm200506/cmbills/009/2006009.htm

Warren S. and Brandies, L. (1890). The Right to Privacy. Harvard Law Review 4(5)

WLIA (2001a) DRAFT WLIA PRIVACY POLICY STANDARDS. Available from the web at http://www.wliaonline.org/publications/.

WLIA (2001b) A DIALOGUE ON PRIVACY ISSUES AND WIRELESS LOCATION SERVICES. Available from http://www.wliaonline.org/publications/argue.html.