2006

Location-Based Services and the Privacy-Security Dichotomy

Katina Michael
University of Wollongong, katina@uow.edu.au

L. Perusco
University of Wollongong

M G. Michael
University of Wollongong, mgm@uow.edu.au

Publication Details

This conference paper was originally published as Perusco, L, Michael, K and Michael, MG, Location-Based Services and the Privacy-Security Dichotomy, in Proceedings of the 3rd International Conference on Mobile Computing and Ubiquitous Networking, London, 11-13 October 2006, 91-98.

Location-Based Services and the Privacy-Security Dichotomy

Abstract
Location-based services (LBS) rely on knowledge of a user's location to provide tailored services or information by means of a wireless device. LBS applications have wide-ranging implications for society, particularly in the context of tracking and monitoring groups of individuals such as children, invalids, and parolees. Despite a great deal of attention paid to technical and commercial aspects of LBS technologies, consideration of the legal, ethical, social and technology momentum issues involved has been wanting. This paper examines some of the more pressing issues that are expected to arise from the widespread use of LBS. The outcome of this paper is the development of an LBS privacy-security dichotomy. The dichotomy demonstrates the importance of striking a balance between the privacy of the individual and national security as a whole. It also presents a realized framework for reasoning about potentially problematic issues in LBS applications.

Keywords
location-based services, privacy, security, ethics, social impacts

Disciplines
Physical Sciences and Mathematics

Publication Details
This conference paper was originally published as Perusco, L, Michael, K and Michael, MG, Location-Based Services and the Privacy-Security Dichotomy, in Proceedings of the 3rd International Conference on Mobile Computing and Ubiquitous Networking, London, 11-13 October 2006, 91-98.

Location-Based Services and the Privacy-Security Dichotomy

L. Perusco,[†] K. Michael[‡] and M.G. Michael*

School of Information Technology and Computer Science, Faculty of Informatics,
University of Wollongong, Northfields Avenue, Wollongong, NSW, 2500, Australia
[†]laura_perusco@iinet.net.au, [‡]katina@uow.edu.au, *mgm@uow.edu.au

ABSTRACT

Location-based services (LBS) rely on knowledge of a user's location to provide tailored services or information by means of a wireless device. LBS applications have wide-ranging implications for society, particularly in the context of tracking and monitoring groups of individuals such as children, invalids, and parolees. Despite a great deal of attention paid to technical and commercial aspects of LBS technologies, consideration of the legal, ethical, social and technology momentum issues involved has been wanting. This paper examines some of the more pressing issues that are expected to arise from the widespread use of LBS. The outcome of this paper is the development of an LBS privacy-security dichotomy. The dichotomy demonstrates the importance of striking a balance between the privacy of the individual and national security as a whole. It also presents a realized framework for reasoning about potentially problematic issues in LBS applications.

Keywords: location-based services, privacy, security, ethics, social impacts.

1 INTRODUCTION

We live in an era of mobility. Mobile technologies, which allow users to move around while maintaining the ability to access a network and its services, now claim a significant degree of attention in both industry and academia [1]. During this time, one particular attribute gains critical importance: location. The ability to pinpoint a mobile user's location creates a new class of applications and services. LBS cover a variety of applications, but all have at least the underlying element in common: they all rely on location knowledge of a user's device to provide tailored services or information. The devices can come in a variety of forms such as a wireless personal digital assistant (PDA) or mobile phone but will increasingly take the form of emerging IP-enabled devices, given the introduction of new protocols and location-aware infrastructure. Examples include in-car GPS navigation, advertising targeted at a mobile phone that enters a particular cell, and remote child monitoring via a GPS-enabled watch.

Potentially LBS has wide-ranging implications for society. In fact, LBS have been described as being "without a doubt one of the most exciting developments to emerge from the mobile telecommunications sector" [2]. However, as newer positioning technologies are introduced into the market with a greater ability to determine location in terms of precision and existing technologies are integrated to overcome limitations, issues pertaining to the use and potential misuse of location information rise to the fore. In addition to this, perhaps because LBS are so new, there has hitherto been limited investigation into exactly what effects the widespread use of these technologies may have. This paper examines the various implications that arise from the use of LBS, including legal, ethical, social and technology momentum issues. The analysis culminates in a discussion and illustrated representation of the LBS trade-off between privacy and security, and the presentation of a realized framework for reasoning about issues in LBS.

2 WHY STUDY POTENTIAL ISSUES ASSOCIATED WITH THE USE OF LOCATION SERVICES?

It is often stated that the changes LBS bring about will be dramatic, with some even going so far as to say that "this technological revolution will directly or indirectly affect in a significant way practically every person in the industrialized world" [3]. LBS are expected to create a radical paradigm shift in the way people live. However, LBS themselves are far more developed than the available research on their potential societal implications. This is clearly not an ideal position for a technical solution which is considered to closely connect with people's private lives, but also with the evident possibility to affect society at large. Thus it is vitally important to consider and provoke debate as to where society is headed with such technological capabilities and innovations. No specific laws and almost no regulations have been written to deal with the possible uses and/ or misuses of LBS. Surely, on the brink of a future where LBS are ubiquitous, one needs to critically speculate on both the unintended effects and consequences.

3 LEGAL AND ETHICAL ISSUES

3.1 Controlling Others

According to Ermann and Shauf, our "ethical standards and social institutions have not yet adapted… to the moral dilemmas that result from computer technology" [4]. Take the example of a woman who uses LBS tracking to watch

over her ailing husband, who has recently survived a heart attack. She is willing to "help" her husband look after himself by monitoring him and restricting the activities she allows him to participate in, especially when he is alone. It is not too difficult to imagine this type of LBS monitoring application becoming commonplace. It is also conceivable that, for some people in such circumstances, the authority to monitor could be held by a hospital or health insurance provider.

What is of utmost importance in this conceivable scenario is that concern for the physical welfare of another person is balanced with their need to be an autonomous being. Consideration of legal issues is also important – it does not appear that countries like Australia or the United States have legislation that covers the unique possibilities that arise from LBS tracking. One situation that is likely to arise with greater frequency is people using LBS technologies to monitor loved ones "for their own good". Several fundamental issues need to be directly addressed as a result. When is a person sufficiently impaired to warrant monitoring? Should their consent be necessary? What if they are considered to be too impaired to make a rational decision about being monitored? These sorts of archetypal questions require urgent resolution as LBS monitoring is predicted to become mainstream. In addition, we could also consider the murky difference between 'monitoring' and 'surveillance' *per se*.

3.2 The Human Need for Autonomy

In most expressions of Western liberalism personal autonomy is considered an integral part of an individual's identity. Resistance to a situation is often unconsciously employed to "preserve psychically vital states of autonomy, identity, and self-cohesion from potentially destabilizing impingements" [5]. If a person's resistance is bypassed or circumvented, their adaptive capacities can be overloaded, inducing feelings of desperation and helplessness. The natural reaction to this is to exert an immediate counterforce in an attempt to re-establish the old balance, or even to establish a new balance with which the individual can feel comfortable.

Autonomy becomes an issue when an individual is closely watched or monitored, and so LBS tracking may have adverse psychological effects on the person being monitored, no matter how well justified that external influence might be. With this in mind, perhaps the only way to implement a monitoring program for an aging individual is to develop a partnership with that person. In this type of arrangement, LBS tracking can be an agreement, i.e. a joint process, that "is continually informed by the goal of fostering … autonomy" [5].

3.3 The Legalities and Ethics of Pre-Emptive Control

Another significant legal and ethical dilemma is that of monitoring people who are suspected of criminal activities or even terrorism, using special court-obtained warrants. This is not mere fancy– the Australian Government for instance, has already passed new anti-terrorism laws that, among other things, give police and security agencies the power to fit terror suspects with tracking devices for up to 12 months [6]. These kinds of powers are particularly problematic. Can it be considered reasonable to impinge upon the freedom of someone who is merely *suspected* of committing a crime? And how much evidence and/ or what type of evidence needs to be gathered in order for a warrant to be issued to authorities? At the present time, ambiguous terminology in both Australian and United States terrorism-related legislation, does not rule out the possibility of authorities using highly invasive chip implant technology to track suspected terrorists.

Criminals surrender a number of their natural rights by committing an offence. By rebelling against society's laws, freedoms such as the right to liberty are forfeited. This is known as retributivism (colloquially known as "just deserts"). The central idea is proportionality: "punishment should be proportionate to the gravity of, and culpability involved in, the offence" [7]. With no crime involved, the punishment of electronic monitoring or home detention must be considered out of proportion.

However, this is not the first instance in which countries similar to Australia have created preventative legislation. In 1994, the *Community Protection Act* was enacted in the state of NSW. This law allowed anyone to be detained in prison for up to 6 months if the Court was satisfied that "the person [was] more likely than not to commit a serious act of violence [that involves a real likelihood of causing death or serious injury, or involves sexual assault], and that it is appropriate, for the protection of a particular person or persons or the community generally, that the person be held in custody" [8]. The first time the law was invoked, it was struck down (to the Government's considerable embarrassment) [9].

The Australian Constitution requires trial by jury for all indictable offences. Is it fair to imprison someone in any way, without due process of law, if they have not committed an indictable offence? Gaudron J's comments about the *Community Protection Act 1994* included the following:

> [T]he proceedings are directed to the making of a guess – perhaps an educated guess, but a guess nonetheless – whether, on the balance of probabilities, the appellant will commit an offence… That is the antithesis of the judicial process [10].

With measures such as those in Australia's new counter-terrorism laws, there is obviously an absolute need for

caution, accountability and review in the exercise of such powers. The London bombings are the justification offered repeatedly by the Prime Minister for the new laws, reinforced by ASIO director-general Paul O'Sullivan. However, this "justification" ignores the reality that "the London bombers were 'clean skins' who had escaped police notice altogether" [11]. Tagging suspicious people cannot keep society completely safe because of the notion of singularities- surprise terrorist attacks that cannot be predicted or prevented using any amount of monitoring or control [12].

The researchers do not make a judgment on whether pre-emptive control legislation is good or bad. It is suggested, however, that the laws developed by the Federal Government (and agreed to by the States) could be indicative of a broader trend. Prime Minister John Howard said that "[i]n other circumstances I would never have sought these new powers. But we live in very dangerous and different and threatening circumstances… I think all of these powers are needed" [13]. Could the same argument be used in the future to justify monitoring everyone in the country? Everyone's privacy being invaded in such a way would likely lower significantly the chance of crimes being committed, or at least the chance of criminals remaining unpunished. If pre-emptive control is a part of government security, then widespread LBS monitoring could be the most effective form of implementation.

Without suggesting an extreme Orwellian scenario where draconian policies and laws mean that the entire population is tracked every moment of their lives, there is a possibility that the current climate is indicative of individuals' willingness to relinquish their privacy (or at least someone else's) for the sake of enhanced security.

4 SOCIAL ISSUES

4.1 Control

Control emerges as a significant theme in LBS. It can be argued that many, if not all, LBS applications have an overarching element of control [14]. Monitoring LBS devices are about controlling others, whether through altruism, pragmatism or necessity. The use of LBS in a business context can be about controlling the types of advertisements that are delivered to a potential customer, and where the person is when they receive those advertisements. An individual's use of a GPS-enabled mobile device is often about control over their own self-direction. Even LBS applications that are ostensibly for care or convenience-related purposes do exhibit aspects of control [15]. In the "husband and wife" example given in section 3.1, the monitoring wife has control over her monitored husband, and in turn this curtails the control the husband exerts over his own life.

4.2 Trust

Trust is a vitally important part of human existence. It develops as early as the first year of life and continues to shape our interactions with others until the day we die [16]. In relationships, a lack of trust means that there is also no bonding, no giving, and no risk-taking [17]. In fact, Marano states:

> Without trust, there can be no meaningful connection to another human being. And without connection to one another, we literally fall apart. We get physically sick. We get depressed. And our minds… run away with themselves [16].

The issue of trust in the use of LBS recalls Perolle's notion of surveillance being practiced in low-trust situations, and the idea that the very act of monitoring destroys trust [18]. Again, this is apparent in the example of the woman who monitors her ailing spouse. She does not trust her husband enough to let him make his own decisions. He probably resents her 24x7 intrusion into his daily activities, but tolerates it out of love and because he does not wish to upset his wife. Their relationship could be expected to become increasingly dysfunctional, if there is a breakdown of trust. It is near impossible to predict the complex effects of LBS when used to track humans in this way, especially as each person has a different background, culture and upbringing. However, if Perolle [18] and Weckert [19] are agreed with, these types of technological solutions may well contribute to the erosion of trust in human relationships– what would this entail for society at large? Freedom and trust go hand-in-hand. These are celebrated concepts which have been universally connected to civil liberties by most political societies.

5 TECHNOLOGICAL ISSUES

5.1 The Technological Momentum of LBS

Some believe that technology is the driving force that shapes the way we live. This theory is known as technological determinism, one of the basic tenets of which is that "changes in technology are the single most important source of change in society" [20]. The idea is that technological forces contribute more to social change than even political, economic or environmental factors.

The present researchers would not go so far as to subscribe to this strongest sense of technological determinism doctrine. The social setting in which the technology emerges is at least as important as the technology itself in determining how society is shaped. As Braun writes: "[t]he successful artifacts of technology are chosen by a social selection environment, [like] the success of living organisms is determined by a biological selection environment" [21]. Technologies that fail to find a market never have a chance to change society, so society shapes

technology at least as much as it is shaped by technology. In this light, Hughes's theory of technological momentum is a useful alternative to technological determinism: similar in that it is time-dependent and focuses on technology as a force of change, but sensitive to the complexities of society and culture [22].

Technological potential is not necessarily social destiny. However, in the case of LBS, it is plausible to expect it to create a shift in the way people live. This shift can already be seen occurring in parents who monitor their children with LBS tracking devices for safety reasons, and in home detention and parole programs that are administered outside prisons to minimize costs and encourage rehabilitation. As described previously, the threat of terrorist attacks has led the Australian Government to bestow upon itself extraordinary powers that never could have been justified previously. In this situation, LBS has enabled the electronic monitoring of suspicious persons, however, it is not the technology alone that acts as the impetus. Pre-emptive electronic tracking could not be put in place without LBS. Neither would it be tolerated without society believing (rightly or not, and at least for an extended period of time) that it is necessary in the current climate. Although technology is not the sole factor in social change, and arguably not the most important, LBS are gaining momentum and are likely to contribute to a shift in the way people live and work.

Table 1: Positives and negatives of LBS for different user types

User Type	**Positives**	**Negatives**
Voluntary user. The most likely type, probably using commercial LBS applications such as in-vehicle routing and navigation.	• Choice. User can opt out of LBS by shutting down, deactivating the device or leaving it in a stationary position. • Safety. Accurate location information may provide timely help in the event of an emergency. • Convenience. E.g. increased ease of routine transactions such as at toll-ways. • Security of the individual. E.g. building access, navigational capabilities.	• Security risk. Even though use is voluntary, the user has a lack of control over who accesses location information. • Privacy risk. Things such as location information and automated transactions can be traced back to the user. • False sense of security. Someone watching from afar cannot necessarily help in an emergency situation such as in the prevention of a kidnapping or attack.
Mandatory user. Possible in the form of government applications (e.g. home imprisonment) and domestic applications (e.g. tracking minors).	• Safety. Personal security may be increased– if someone can see where the user is at all times. • Accountability. Location can be monitored constantly, so the user may be held responsible for their activities. If a crime is committed, they may be implicated or cleared based on location information. • Security of society. The user's knowledge that someone can see their every move may prevent them from taking part in a criminal activity.	• Invasion of privacy. Location can be viewed at any time, with or without user consent. • Security risk. Location information is constantly available, so data leaks are potentially very serious. • Decreased autonomy. Independence is important to mental and emotional wellbeing. • May give user a false sense of security. Someone watching from afar cannot necessarily prevent harm to another. • May give society a false sense of security. Monitoring does not mean that a crime cannot be committed.
Non-user. Unlikely to be a large group if LBS become widespread. Many in this category would have personal reasons for not adopting LBS, or could not afford to use the technology.	• Privacy. Personal location information remains relatively protected. • Autonomy. High level of independence and control over their own activities. • Simplicity. There is no need to deal with the possibility of the technology failing.	• Safety risk. Help may be delayed in the event of an emergency, although programs like E911 now mean that emergency services can pinpoint a caller's location with an accuracy of between 50 and 300 meters [24]. • Security risk. The person's activities may pose a danger to society, community misses out on the security benefits of LBS. • Risk of prejudice. A person may be suspected of wrongdoing without evidence, simply by reason of opting-out of LBS.

5.2 Technology Is Not Infallible

If LBS do become an integral part of daily life, it must be considered what will happen in the instances that the technology will inevitably fail- whether it fails to record location data properly, provides inaccurate measures, is accessed by unauthorized persons, or the secondary support systems fail. No technology is *fail-safe*. There are invariably shortcomings, limitations, and the unforeseen. An example is the use of electronic monitoring in parole and home imprisonment programs. One U.S. study found that about 75 percent of electronically monitored "walk offs" were re-apprehended within 24 hours [23]. That means a quarter of these people went free for more than a day– sufficient time to commit other offences. And, although the offender may be caught and punished, it is difficult to remedy the damage committed to a victim of crime.

6 EVALUATING LBS

Any technology can be expected to typically have both positive and negative effects on individuals and on the wider community. Emmanuel Mesthane of Harvard's former Technology and Society Program wrote: "[n]ew technology creates new opportunities for men and societies and it also generates new problems for them. It has both positive and negative effects and it usually has the two at the same time and in virtue of each other" [25]. The assets and liabilities that flow from LBS (to the individual involved and to society as a whole) depend largely on whether the person using the technology does so of their own accord, or is required to use it for one reason or another. There are a different set of pros and cons related to people who do not use LBS at all. Some of the benefits and drawbacks for voluntary, mandatory and non-users of LBS are presented in Table 1.

7 RISK TO THE INDIVIDUAL VS. RISK TO SOCIETY

From Table 1, it is obvious that there is an inherent trade-off between the interests of the individual and the interests of society as a whole: the privacy of the individual is in conflict with the safety of the broader community. As G.T. Marx reflects, "[h]ow is the desire for security balanced with the desire to be free from intrusions?" [26] This work is certainly not the first to allude to this issue. For example, Kun has said that "perhaps one of the greatest challenges of this decade will be how we deal with this theme of privacy vs. national security" [27]. The original contribution of this paper is that the dilemma has been related specifically to LBS, under the privacy-security dichotomy. Here, each side of the dichotomy is divided into three key components that combine to greatly magnify risk. Sections 7.1 and 7.2 describe the factors present in each dichotomy. Removing one or more components for each set decreases the privacy or security risk. Where more elements are present in conjunction, the risk is increased.

7.1 Privacy Risk

Significant privacy risk occurs when the following factors are present:

- *Omniscience*– LBS tracking is mandatory, so authorities have near-perfect knowledge of people's

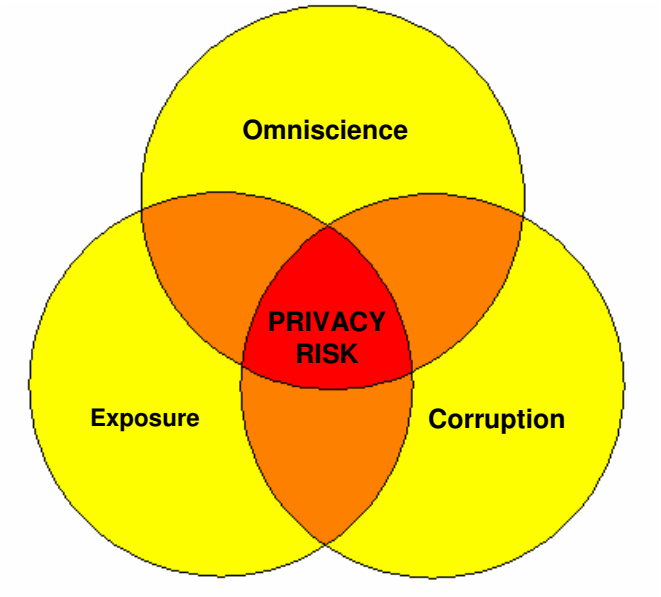

Figure 1: Privacy risk

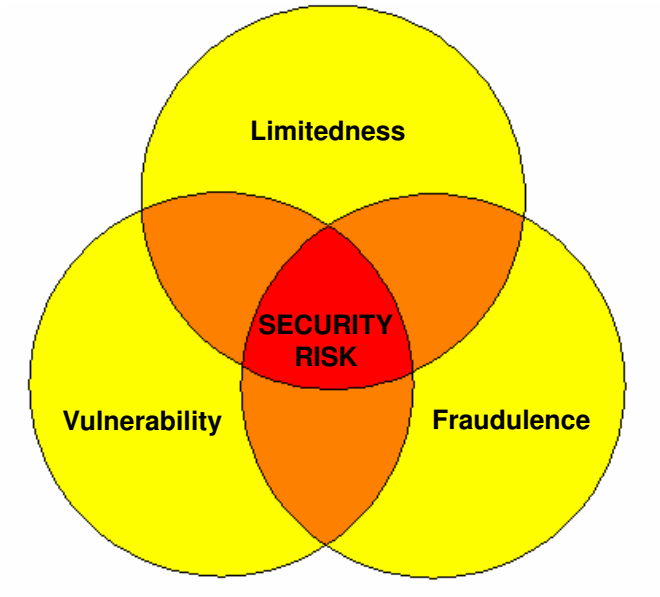

Figure 2: Security risk

whereabouts and activities.

- *Exposure*– security of LBS systems is imperfect, leaving them open to unauthorized access.
- *Corruption*– motive exists to abuse location-related data. This includes unauthorized or improper changes, thus compromising content integrity.

It is not difficult to see why the danger in this privacy-risk scenario is so great. A nation with all-knowing authorities means that a large amount of highly sensitive information is stored about all persons in the country. Security of electronic systems is never completely foolproof. And, where there is something to be gained, corrupt behavior is usually in the vicinity. The combination of all three factors creates a serious threat to privacy.

7.2 Security Risk

Significant security risk occurs with the following conditions:

- *Limitedness*– authorities have limited knowledge of people's activities.
- *Vulnerability*– security of individuals and infrastructure is imperfect.
- *Fraudulence*– motive exists to commit crimes.

This security-risk dimension is a life situation which people have to contend with in the present day: limitedness, vulnerability, and fraudulence. Law enforcement authorities cannot be everywhere at once, nor can they have instant knowledge of unlawful activity. Security of infrastructure and people can never be absolute. In addition to this, there are always people willing to commit crimes for one reason or another. These factors merge to form a situation in which crimes can be committed against people and property relatively easily, with at least some chance of the perpetrator remaining unidentified.

7.3 How Much Are We Willing to Compromise?

As mentioned above, the security-risk half of the dichotomy typifies our current environment. However, the majority of society manages to live contentedly, despite a certain level of vulnerability and the modern-day threat of terrorism. The security-risk seems magnified when examined in the context of the LBS privacy-security dichotomy. LBS have the potential to greatly enhance both national and personal security, but not without creating a different kind of threat to the privacy of the individual. The principal question is: how much privacy are we willing to trade in order to increase security? Is the privacy-risk scenario depicted above a preferable alternative to the security-risk society lives with now? Or would society lose more than it gains? And how are we to evaluate potential ethical scenarios in the context of utilitarianism, Kantianism, or social contract theory?

8 RESOLVING THE ISSUES

This paper has already identified four types of issues associated with LBS: legal, social, ethical and technological. From the preceding information, we can begin to see one overriding theme for each of these issues:

- Legal– control of others, with or without their

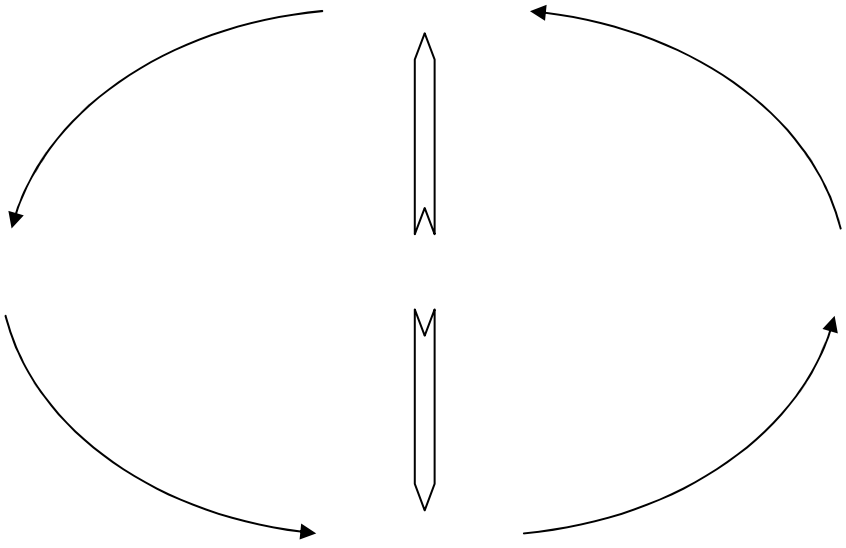

Figure 3: Relationships between major issues in LBS

Table 2: Issues framework for LBS

Privacy	**Control**
• Who has access to location information? • Can an individual wearing a tracking device deactivate it? • Do the benefits that accrue from LBS in a given context outweigh the impacts of seriously invading an individual's privacy? • Is this individual's privacy worth more than the safety and security of society?	• Who is controlling whom, and for what reasons? • Does the person to be monitored need to consent? • Is an individual too impaired to consent to their own monitoring? If so, who should be able to make the decision for them? • If an individual does not consent to monitoring, are there special circumstances (e.g. an indictable crime), that warrants control without consent? • How can it be ensured that inaccuracies in reported location do not adversely affect the individual being monitored?
Security	**Trust**
• What restrictions are placed on organisations (and their employees) that handle location information? • How well protected are the LBS electronic systems and subsequent support systems? • What measures are in place to manage mandatory LBS users? • What backup measures are in place in case the system fails?	• Does the LBS context already involve a low level of trust? • If the LBS context involves a moderate to high level of trust, why are LBS being considered anyway? • Will the use of LBS in this situation be trust-building or trust-destroying?

consent
- Social– trust in human relationships
- Ethical– privacy of the individual
- Technological– security and reliability of LBS systems

These four major issues can be summarized as control, trust, privacy and security.

8.1 Relationships Between Control, Trust, Privacy and Security

The issues of control, trust, privacy and security are interrelated. As discussed above, increased control can impinge or even destroy trust. I.e. there is no need to be concerned with trusting someone when you can monitor them from afar. In contrast, increased trust would normally mean increased privacy. An individual who has confidence in another person to avoid intentionally doing anything to adversely affect them, probably does not feel the need to scrutinize that person's activities.

Privacy requires security as well as trust. A person's privacy can be seriously violated by a security breach of an LBS system, with their location information being accessed by unauthorized parties. The other effect of system security, however, is that it enhances control. A secure system means that tracking devices cannot be removed without authorization, therefore, control is increased. Of course, control and privacy are mutually exclusive. Constant monitoring destroys privacy, and privacy being paramount rules out the possibility of LBS tracking. These relationships are summarized in Figure 3.

8.2 Guiding Deliberation

The above discussion of latent and realized concerns in LBS underscores the following question: with the lattice of issues involved and the potentially dangerous implications of not taking these into account, how *should* LBS be used? Mason and Mason et al. developed a framework of questions for reasoning about ethical issues in electronic commerce [28]. The researchers suggest the use of a similar framework for discussion and thought on the most critical issues in implementing LBS [29]. This would go some way toward overcoming the difficulty of using LBS both lawfully and properly. Table 2 presents this original framework, derived from information presented previously in this paper.

9 CONCLUSION

This paper has examined the major legal, ethical, social and technological issues involved in the use of LBS. It has been shown that the benefits and drawbacks of LBS (for both the individual and for society) largely depend on the type of user and given context. The outcome of this paper is in its LBS-specific examination and diagrammatic representation of the dichotomous relationship between the privacy of the individual and the security of society. Another key attainment presented here is the LBS issues

framework which includes privacy, control, security and trust.

LBS are beginning to make their way into the mainstream. However, it seems that there has been little consideration of the possible implications of these technologies, particularly compared to the degree of attention that technical and commercial aspects of LBS have received. With the very real potential of LBS to create social change it is vitally important to begin looking at why LBS should be used in certain contexts and to address the social, legal, ethical and technological issues that arise from the technology's implementation. The recommendations are to go beyond socio-ethical guidelines (themselves crucially important), and to implement fair-practices, standards and regulations that determine what can and cannot be achieved using LBS by any number of stakeholders in the value chain.

REFERENCES

[1] G.M. Giaglis, G.M., P. Kourouthanassis, and A. Tsamakos, Towards a Classification Framework for Mobile Location Services, in B.E. Mennecke, and T. Strader (eds), Mobile Commerce: Technology, Theory and Applications, pp. 67-68 (2003).

[2] K. Mitchell, and M. Whitmore, Location Based Services: Locating the Money in B.E. Mennecke, and T. Strader (eds), Mobile Commerce: Technology, Theory and Applications, pp. 51, 53 (2003).

[3] B.E. Mennecke, and T. Strader (eds), Mobile Commerce: Technology, Theory and Applications, p. vii (2003).

[4] M.D. Ermann, and M.S. Shauf (eds), Computers, Ethics and Society, p. vi (2003).

[5] E. Adler, and J.L. Bachant, Intrapsychic and Interactive Dimensions of Resistance: A Contemporary Perspective, Psychoanalytic Psychology, Vol. 15, No. 4, pp. 451, 454 (1998).

[6] N. Gilmore, PM Defends Anti-terrorism Laws, *Lateline* (September 8, 2005) <http://www.abc.net.au/lateline/content/2005/s1456384.htm> [Accessed Sept 22, (2005)].

[7] D. Brown, D. Farrier, S. Egger, and L. McNamara, Criminal Laws, p. 1376 (2001).

[8] Community Protection Act 1994 (NSW) s5.

[9] E. Handsley, Public Confidence in the Judiciary: A Red Herring for the Separation of Judicial Power, Sydney Law Review, June, Vol. 20, No. 2, p. 183 (1998).

[10] *Kable v Director of Public Prosecutions* (1996) HCA 24. Available through AUSTLII [Accessed September 27, (2005)].

[11] M. Wilkinson, Powers Pave Way for Secret New World, The Sydney Morning Herald, (September 28) pp. 1, 6 (2005).

[12] I.O. Angell, Can Technology Manage Identity?, Public Lecture at the University of Wollongong, 17th July 2006.

[13] J. Kerr, House Arrest for Terror Suspects, The Sydney Morning Herald (September 28) p. 1 (2005).

[14] A. Masters, and K. Michael, Lend Me Your Arms: the Use and Implications of Humancentric RFID, Electronic Commerce Research and Applications, in press (2006).

[15] A. Masters, and K. Michael, Humancentric applications of RFID implants: the usability contexts of control, convenience and care, The Second IEEE International Workshop on Mobile Commerce and Services 19th July: Munich, Germany, IEEE Computer Society, Washington, pp. 32-41, (2005).

[16] H.E. Marano, Trust Someone, Again, Psychology Today, Jul/Aug, Vol. 31, Iss. 4, p. 7, (1998).

[17] T. Mizrahi, How Can You Learn to Trust Again?, Psychology Today, Mar/Apr, Vol. 35, Iss. 2, p. 12, (2002).

[18] J.A Perolle, Computer-Supported Cooperative Work, in D. Lyon, and E. Zureik (eds), Computers, Surveillance and Privacy, pp. 47, 59 (1996).

[19] J. Weckert, Trust and Monitoring in the Workplace, IEEE International Symposium on Technology and Society, p. 245, (2000).

[20] L. Winner, Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought, p. 76, (1977).

[21] E. Braun, Futile Progress: Technology's Empty Promise, p. 21, (1995).

[22] T.P. Hughes, Technological Momentum, in M.R. Smith, and L. Marx (eds), Does Technology Drive History? p. 101, (1994).

[23] NLECTC, Keeping Track of Electronic Monitoring, National Law Enforcement and Corrections Technology Center Bulletin (Oct. 1999) <http://www.justnet.org/pdffiles/Elec-Monit.pdf> [Accessed September 25, (2005)].

[24] Federal Communications Commission, Enhanced 911 (June 17, 2005) <http://www.fcc.gov/911/enhanced/> [Accessed October 11, (2005)].

[25] P. Bereano, Technology Is a Tool of the Powerful, in M.D. Ermann, and M.S. Shauf (eds), Computers, Ethics and Society, p. 85, (2003).

[26] G.T. Marx, Electric Eye in the Sky: Some Reflections on the New Surveillance and Popular Culture, in D. Lyon and E. Zuriek (eds), Computers, Surveillance and Privacy, p. 195, (1996).

[27] L.G. Kun, Homeland Security: The Possible, Probable and Perils of Information Technology, IEEE Engineering in Medicine and Biology, Sept/Oct, Vol. 21, Iss. 5, pp. 28, 31, (2002).

[28] E. Turban, D. King, J.K. Lee, and D. Viehland, Electronic Commerce: A Managerial Perspective 2006, p. 735, (2005).

[29] K. Michael, A. McNamee, and M.G. Michael, The Emerging Ethics of Humancentric GPS Tracking and Monitoring, International Conference on Mobile Business, 25th-27th July: Copenhagen, Denmark, IEEE Computer Society, Washington, (2006).