2006

Location-based services and the price of security

Holly Tootell
University of Wollongong, holly@uow.edu.au

Location-based services and the price of security

Abstract

Location-based services (LBS) are one of many high- tech solutions to national security, providing advanced information capabilities. With their use comes a perceived increase in citizens having reduced access to services and information as well as waiving certain liberties in order for national security initiatives to be fully implemented. Focusing particularly on the role of LBS, this research will establish an understanding of the 'price' people pay for national security when it is achieved using LBS. The exchange of liberties for security will be illustrated by the results of the content analysis. This research provides insight in to how far a location- based technology can be utilized in national security applications before its perceived cost-benefit is exceeded.

Disciplines

Physical Sciences and Mathematics

Publication Details

Tootell, H. (2006). Location-based services and the price of security. International Symposium on Technology and Society (pp. 1-6). Piscataway, NJ, USA: IEEE.

Location-Based Services and the Price of Security

Holly Tootell
University of Wollongong, Australia
holly@uow.edu.au

Abstract

Location-Based Services (LBS) are one of many high-tech solutions to national security, providing advanced information capabilities. With their use comes a perceived increase in citizens having reduced access to services and information as well as waiving certain liberties in order for national security initiatives to be fully implemented. Focusing particularly on the role of LBS, this research will establish an understanding of the 'price' people pay for national security when it is achieved using LBS. The exchange of liberties for security will be illustrated by the results of the content analysis. This research provides insight in to how far a location-based technology can be utilized in national security applications before its perceived cost-benefit is exceeded.

1. Introduction

Whether it is the use of RFID bracelets to monitor home-detention prisoners, the implementation of biometric identification passport systems or the development of GPS monitoring systems for natural disaster management, the notion that personal privacy and liberty will be affected in order to enhance security cannot be denied.

The advancement of location based services (LBS) has ensured that privacy and liberty are going to be affected in order to achieve the levels of national security that have become such a focus for governments globally. Previous studies in the area of LBS and national security have focused on the implementation of a single technology, or, on the privacy impact of one technology. This has created difficulties for researchers wanting to study the continually changing response of the public to LBS.

2. RFID and national security: social perspective

The advantages of LBS technologies are well-researched. Take for example the use of Radio Frequency Identification (RFID). The following section introduces some of the key concerns of this research regarding privacy and liberty. "RFID has tremendous potential for improving productivity and security, but it will also become one of the touchstone privacy issues of our times" Senator Patrick J. Leahy [1]. RFID is a method of automatic identification and is a generic term for technologies that use radio waves to automatically identify entities; either live or inanimate. RFID has been referred to by some as the new barcode implying a new era of automatic identification is emerging.

The beginnings of RFID can be traced back to World War II and the Early Identification Friend or Foe system that enabled friendly aircraft to respond to a correct signal, protecting them from being shot down [2]. Although research began into RFID in the 1970s, its commercial applications only began to be realised from the early 1980s onwards [3, 4]. RFID has been in use for a number of years for applications like military equipment tracking and large shipping containers, but the cost drop to a few cents has widened the scope for use in recent times.

Some of the more common examples of applications include: baggage tracking in airports, supply chain management and supply chain theft reduction, remote keyless entry for automobiles, animal tracking, highway toll collection, and passport security. For airport baggage identification, RFID has eliminated the need for manual sorting and lifting and is claimed to have enhanced passenger security [5]. Highway toll collection using RFID has allowed drivers the convenience of driving straight through checkpoints without needing small change [6, 7]. The inclusion of RFID tags in passports and possibly drivers' licenses acts as an 'anti-counterfeiting feature [8].

Since 9/11 the threat of terrorism has ensured that the tracking offered by RFID is a favored system implemented to alleviate that threat be it in shipping containers or passport control. Atkinson [6] observed that prior to 9/11 the use of RFID was limited to supply chain security and loss prevention, however in the post-9/11 world, the focus for RFID is ensuring tamper-proof containers due to terrorism concerns.

1-4244-0479-7/06/$20.00 ©2006 IEEE

In emergency response situations, like the 2004 Boxing Day Tsunami RFID tags have assisted in management and location identification of survivors as they are moved between emergency housing facilities. Alternatively they have assisted in mass-casualty victim identification management.

2.1. Acceptance of the increasing pervasiveness of technology

Without the perspective of national security, it is still easy to find examples of innocuous, everyday technologies that are becoming more and more pervasive. The humble mobile phone was once solely a telecommunications device that allowed the convenience of telephone calling from wherever it was you were. Convergence has meant that the same phone is now a still camera, a video camera, a PDA, an mp3 player, a game device, a GPS device, a television, email access point, internet connection, a voice recorder and note taker, a digital storage device, and a radio. Not only that, its significance as a location device is reflected in emergency response laws that mandate that the caller's location can be determined by the geographic location of the cellular phone within 100 meter accuracy. There are other examples of mobile phones being used for location purposes: good shopping deals, recommended restaurants in a specific area, traffic information, and find a friend functions. As a small sample of available functionality, these reflect the level of pervasiveness mobile phones now have in our lives. Although not every subscriber would use these functions, they are fast becoming an integral part of the way we conduct both personal and business tasks.

Each of these functions, when considered singly, provide a benefit to society by increasing convenience, speed of processing or enhancing security; however, the threats of function creep does leave open an opportunity for surveillance that is enabled by the technology. Advocates of the technology will dismiss the significance of tracking as a necessary side-effect of using the technology. Privacy-focused studies have identified LBS technologies as being perceived as a threat to privacy regardless of purpose [9]. They have also examined the change in public perception to information collection and management for the purpose of 'homeland' security [10, 11].

It is to be remembered that the purpose of this research is to examine in detail the issues raised by technology and privacy advocates. It is not to assign moral correctness or incorrectness to the actions of adopters of the technology, but to provide an evidence-based argument of the true social cost of these technologies.

3. Understanding the Price of Security

The price of security is not a monetary value that can be calculated. The price of security is a figurative concept that looks to explain the impact of location based services on the privacy and liberty aspects of life. The use of technologies to help ensure national security levels are maintained is, more often than not, a decision that is made by governments, and not a personal one. Therefore individuals do not often have the option of refusing to adopt the technology. The following section provides an observation of privacy and the concept of price of security before and after the tragic events of 9/11. It is that date that forever changed western governments' approach to national security protection.

3.1. Notion of privacy before 9/11

Privacy is a concept that has eluded a single, clear definition [12]. McLean likens privacy to the concepts of liberty and freedom: each a concept unable to be easily defined. Privacy has been recognized as a concept that has evolved with the progress of society, changing to suit the demands of the current times. Warren and Brandeis [13] first wrote of the right of privacy in 1890, asserting that privacy was the right to be left alone. Clarke [14] prefers not to assume privacy is a right: as a right implies an intrinsic and absolute standard, something not always applicable to privacy. Recognizing privacy as an interest that an individual sustains, allows for a more flexible definition that suits the application of privacy in both the offline and online environment. The recognition of the right to privacy is deeply rooted in history and can be identified in the Bible, in traditional Jewish law and in classical Greek and ancient Chinese societies[3].

Privacy has been considered to be an important concept over a long period of time; however it is in the recent past that it has risen to a higher level of interest. This can be attributed to the increase in database systems collecting information about us [15] or it can be likened to the concepts of 'dataveillance' or 'panoptic sort' described by Clarke [14] and Gandy [16] accordingly. Both these terms relate to the ability of collections of information to be equated with power. The increase in technological capability over the past few decades has seen an increase in the potential of machines and systems to collect and relate data about ourselves. The transition to an online economy, or at the very least, online commerce, has created a whole new pool of information to be collected tracked and stored. Clarke [14] and Gandy [16] recognized that collection of data was occurring well before the online world came into existence.

The introduction of online communications, and more particularly electronic transactions and enormous increase in storage capacity, has resulted in a changing attitude to control of privacy.

3.2. Notion of privacy after 9/11

"If you have nothing to hide… you have nothing to fear." [17] Lyon is a strong proponent of this never having been the case and even less so in the post-September 11 environment where surveillance has often been undertaken without clear and democratically defined limits [17].

"The attacks brought to the surface a number of surveillance trends that had been developing quietly and largely unnoticed, for the previous decade and earlier." [17]. Lyon believes that the events of 9/11 provided a plausible reason for deploying a number of surveillance schemes, which until that point, had not had a valid reason for being used.

Privacy, after 9/11, has proven to be the scapegoat of anti-terror campaigners, and governments wanting to establish more severe surveillance measures. It appears that if privacy can be squashed, then the fight against terror will be much stronger. It is proposed that a trend to support this will be found in analysis of popular media. Preliminary investigations have been supported by discussions at a recent Australian summit on terrorism legislation.

With a heightened awareness of privacy generally, new technology applications that are proposed are more closely scrutinized by the public. One of the major causes for concern about privacy is a lack of understanding of exactly what the technology can do and what it is proposed to be used for [18]. The level of fear after 9/11 is raised by Lyon [19] as dominant theme for an increase in surveillance, which in turn has raised awareness levels of privacy advocate groups.

3.3. Defining of the Price of Security

To understand the concept of price of security, there are two views that can be investigated: firstly that an exchange or trade-off that is mutually acceptable takes place, or that a citizen is giving up or losing rights altogether under the guise of a 'greater good'.

The concept of exchange is more palatable to those charged with enforcing changes. Exchange implies "the act or an instance of giving one thing and receiving another in its place" [20]. In terms of the price of security, this is where the public is made aware of the necessity for change for direct protection benefits. This has been seen in the case of airline travel. Security checks have higher levels of scrutiny, which in many cases has caused passengers to add an amount of time to their travels. The exchange that has taken place here is time for safe travel. The majority of passengers have agreed that this is a worthwhile exchange.

The second view of price of security is that there is a loss, or some aspect of personal liberty has been given up. Loss can be considered as something that you can "be deprived of or cease to have" [21]. In this instance the public is made aware of changes that are taking place, but no reason is given that warrants the change, and no benefit is received in return. This is described well by Halchin [22, 23] who has examined the use of government websites by terrorist organizations as an aid to planning attacks. From this aspect, control and management of information is seen as critical to the fight to protect national security. However by restricting access to online government information, ordinary citizens, without ulterior motives have lost the freedom to conduct their transactions with governments.

Anecdotal evidence suggests that the concept of loss or giving up of liberties is a more acceptable proposal to sell to a worried public fearful of imminent terror threats. It is only after the imminent threat has passed that the concept of exchange is more fully investigated.

4. Contribution of this research

The point of this research is to find the trade-off that takes place between privacy and security. The content analysis will identify evidence to support the claim that there is a shift between loss and exchange as the time from the terror event passes. Again, through anecdotal observation, it has been seen that governments and citizens alike have unplanned, emotional responses directly following an event of national security significance. This is understandable, however, through the application of critical social theory, outlined below, it is hoped a state of emancipation will be attained that encourages a period of reflection before changes are put in place.

5. Method

To understand the motivations of government and drivers for public motivation and adoption, Critical Social Theory (CST) developed by Jurgen Habermas [24, 25] is applied. The primary objective of CST, and more particularly the application of CST to Information Systems (IS) research is to discover how "…many small IT changes add up to a policy that affects the nature of the society in which we live" [26]. CST's primary aim is emancipation through knowledge and study of past behavior. CST allows the issue of LBS adoption for national security to be studied by examining events of national security significance through public reaction as documented in popular media.

Content analysis has gained momentum as a research method through the rapid expansion of mass communication, both mass media and international politics [27]. Content analysis is useful for making inferences by objectively and systematically recognizing particular patterns within messages.

The content analysis will be used to verify the anecdotal observations that suggests at selected time periods after an event of national security significance, public sentiment changes to reflect a more learned appreciation of measures that have taken place in response to the event. Through performing multiple analyses of the same data sets but focusing on specific indicators eg: event, time period, or technology, indicators of change will be able to be extracted and compared.

The analysis phase of the research is two-fold. The initial analysis is quantitative and captures counts of newspaper headlines and leading paragraphs based on specific national security events with a set of key terms to link to the concept of price of security. The second component will use content analysis software to observe the pattern of feeling described in the newspaper reports. Analysis of newspaper headlines is an established method for studying issues, especially when the researcher is concerned with uncovering trends and perception of social implications [28].

6. Comparison of Pilot Study Results

The pilot study has restricted investigations to two events: September 11 terrorist attack in the United States that occurred in 2001, and the Bali bombing that occurred on October 12, 2002. The results that appear below are looking for trends in reactions from global newspaper sources. The counts of headlines from newspapers around the world allow the first understanding of the depth of effect of each of the events.

6.1. Quantitative Results

The results in Figure 1 show the number of headlines associated with September 11 and the concept of security and terrorism in the twelve months after the attack. The trend shows that after the initial shock of the event, there is a significant decline in the number of headlines being reported. At the nine month mark after the occurrence of the event attention starts to increase again.

Figure 2 shows the same analysis of headlines for the first twelve months after the Bali bombing. The same pattern is found, where after initial shock is dispersing, there is a short period of time before attention begins to build again.

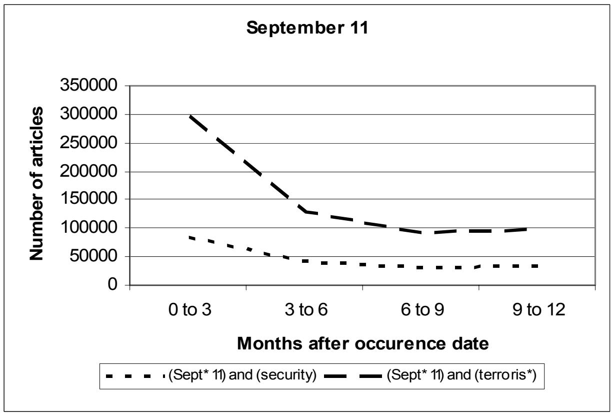

Figure 1. Headlines about 9/11 and security and terrorism

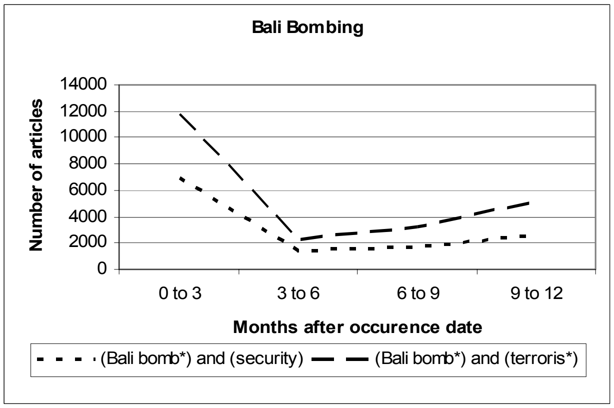

Figure 2. Bali bombing headlines

Figure 3 shows the results for trends in 9/11 and Bali bombing reporting with regard to LBS and privacy using a longer time period for the sample of headlines than the previous two. The trend lines indicate that there is a definite pattern in response in the media following a terror event. The second phase of analysis of the research will look in depth at specific time periods that are of interest. At the six month mark, there is an increase in both the 9/11 and Bali data; the first anniversary of the events is significant not only for survivors and memorial events, but also as a checkpoint for those introducing measures to prevent the events occurring again.

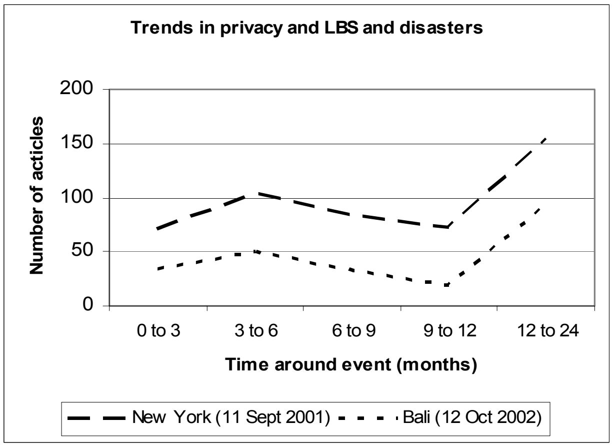

Figure 3. Privacy and LBS trends

6.2. Issues apparent in findings

From the three figures, it can be seen that there are trends that need investigation. They are behaving in an expected pattern that confirms the anecdotal observations made by the researcher. The results of the initial phase of investigation are justification for the second phase of the research. The trends identified in the first phase will form the basis for the content analysis. Through the investigation of these trends, reasons and public sentiment will be uncovered. The content analysis of articles at the time of interest will give a deeper understanding of the reactions to events; especially the introduction of new laws, technologies or social implications.

6.3 Future directions of study

In its entirety this research will analyze each of the events specified in Table 1. By investigating each of these cases across terror events, natural disasters and disease outbreaks, recurrent patterns of reaction are expected to be found. By better understanding the patterns of reaction, emancipation from past events can be achieved.

Table 1. List of events

Event	Date
New York	11-Sep-2001
Bali Nightclub Bombing	12-Oct-2002
Jakarta Embassy Bombing	9-Sep-2004
London Train and Bus Bombing	7-Jul-2005
SARS	1-Jan-2003
Asian Tsunami	26-Dec-2004
Hurricane Katrina	29-Aug-2005

7. Conclusion

If location-based services are to be used for national security initiatives then it will be necessary to understand the implications they will have on the liberty and privacy of the people they are being used to protect. Identifying patterns of reaction to adoption of the technologies will help people understand the exchange or loss that will take place. The concept of price of security is one mechanism that will be able to be used to weigh the benefits of a new technological solution against the impact it will have on privacy and liberty.

At the beginning of this research project the author was aware of patterns being seen in response to terror events and the subsequent legal, technical and social reactions. To bring these aspects together will provide a strong basis for proving that there is a price of security. It is the interlinking of these components that gives us the complexity and richness of the society we live in. One component cannot be understood without the others.

8. References

1. Swartz, N., *Tagging Toothpaste and Toddlers.* Information Management Journal, 2004. **38**(5): p. 22.

2. Garfinkel, S.L. and H. Holtzman, *Understanding RFID Technology*, in *RFID: applications, security and privacy*, S.L. Garfinkel and B. Rosenberg, Editors. 2006, Pearson Education, Inc.: New Jersey. p. 15-36.

3. Jones, P., et al., *Radio Frequency Identification in Retailing and Privacy and Public Policy Issues.* Management Research News, 2004. **27**(8/9): p. 46.

4. Pierce, A., *Radio Frequency Identification Tags.* Tech Directions, 2004. **63**(6): p. 11.

5. Anonymous, *Florida airport gets first RFID system.* IIE Solutions, 2002. **34**(7): p. 14.

6. Atkinson, W., *Tagged: The Risks and Rewards of RFID Technology.* Risk Management, 2004. **51**(7): p. 12.

7. Garfinkel, S.L., A. Juels, and R. Pappu, *RFID privacy: an overview of problems and proposed solutions.* Security & Privacy Magazine, IEEE, 2005. **3**(3): p. 34-43.

8. Smith, L., *RFID Report.* The Humanist, 2005. **65**(3): p. 37.

9. Strickland, L.S. and L.E. Hunt, *Technology, security, and individual privacy: New tools, new threats, and new public perceptions.* Journal of the American Society for Information Science and Technology, 2005. **56**(3): p. 221-234.

10. Feinberg, L.E., *FOIA, federal information policy, and information availability in a post-9/11 world.* Government Information Quarterly, 2004. **21**(4): p. 439-460.

11. Meeks, B.N., *Conspicuous in their silence - Where are the voices defending the very fought-after privacy rights now threatened in the name of Homeland Security?* Communications of the Acm, 2003. **46**(2): p. 15-16.

12. McLean, D., *The Difficulty of Privacy as an Idea*, in *Privacy and its Invasion*. 1995, Praeger Publishers: Westport. p. 1-7.

13. Warren, S.D. and L.D. Brandeis, *The Right to Privacy.* Harvard Law Review, 1890. **4**(5): p. 193.

14. Clarke, R. *Introduction to Dataveillance and Information Privacy, and definitions of terms*. 1997 [cited; Available from: http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.

15. Garfinkel, S.L., *Database nation : the death of privacy in the 21st century*. 2000, Beijing: O'Reilly.

16. Gandy, O.H.J., *The Panoptic Sort: A political economy of personal information*. 1993: Westview Press.

17. Lyon, D., *Surveillance after September 11*. 2003, Malden, Massechusetts: Polity Press in association with Blackwell Pub. Inc.

18. Organisation for Economic Co-operation and Development, *The security economy*. 2004, Paris: OECD.

19. Lyon, D., *Surveillance Technologies: Trends and Social Implications*, in *The Security Economy*, O.f.E.C.-o.a. Development, Editor. 2004, OECD: Paris. p. 127-148.

20. The Australian Oxford Dictionary. *"exchange n."* 2004 [cited 2006 15 May 2006]; 2nd edition:[Available from: <http://www.oxfordreference.com/views/ENTRY.html?subview=Main&entry=t157.e18656>.

21. The Australian Oxford Dictionary. *"lose v."* 2004 [cited 2006 15 May 2006]; 2nd edition.:[Available from: <http://www.oxfordreference.com/views/ENTRY.html?subview=Main&entry=t157.e31959>.

22. Halchin, L.E., *Electronic government: Government capability and terrorist resource.* Government Information Quarterly, 2004. **21**(4): p. 406-419.

23. Halchin, L.E., *Electronic government in the age of terrorism.* Government Information Quarterly, 2002. **19**(3): p. 243-254.

24. Habermas, J., *Communication and the evolution of society / Jurgen Habermas ; translated and with an introduction by Thomas McCarthy*. 1979, London :: Heinemann,.

25. Habermas, J., *The theory of communicative action*. 1984, Boston :: Beacon Press,.

26. Klein, H.K. and M.Q. Huynh, *The Critical Social Theory of Jurgen Habermas and its Implications for IS Research*, in *Social Theory and Philosophy for Information Systems*, J. Mingers and L. Willcocks, Editors. 2004, John Wiley & Sons Ltd.: West Sussex, England. p. 157 - 237.

27. Titscher, S., et al., *Methods of Text and Discourse Analysis*. 2000, London: SAGE Publications.

28. Zamoon, S. and S. Curley, *Ripped from the Headlines: What Can Popular Press Teach us about Software Piracy?* 2006, Management Information Systems Research Center, Carlson School of Management, University of Minnesota: Minneapolis.