Prometheus, Vol. 24, No. 4, December 2006

The Application of Critical Social Theory to National Security Research

HOLLY TOOTELL

Abstract *High-tech solutions to national security, specifically Location-Based Services (LBS), are attracting increased attention from citizens as they become more pervasive. The connection between LBS and national security has been made in previous ICT studies but has been limited to either the technological or the privacy impact of LBS. They have not addressed the use of LBS from a 'lifeworld' perspective. To do this Habermas's Critical Social Theory (CST) is proposed as a method suitable for investigating the social impact of the technologies and identifying factors driving governments to adopt such technologies. The theory is applied to the national security context.*

Keywords: national security; critical social theory; location-based services; IS research; content analysis.

1. Introduction

This study seeks to examine the relationship that exists between the use of location-based services (LBS) and national security initiatives, and specifically the perceived impact they have on citizens.

Public awareness of national security has increased significantly since the terrorist attacks in the United States of America on September 11, 2001. Of the many high-technology solutions used in response to breaches of national security the use of complex information technologies, including radio frequency identification (RFID), global positioning system (GPS), and biometric identification appear to be the most popular. Location-based services require these technologies to provide functions that include: immigration and visa control applications (through biometric identification on passports) to advanced home-detention functionality (RFID chips for movement tracking).[1] Location applications have the potential to be privacy insensitive and pervasive, and are already considered by some to be inherently so.[2] Evidence suggests that there is a need to research the impact that location applications have on society as a whole.

Prometheus ISSN 0810-9028 print/ISSN 1470-1030 online © 2006 Taylor & Francis
http://www.tandf.co.uk/journals
DOI: 10.1080/08109020601029995

Previous studies of LBS with respect to national security have focused on two main categories: technology responses to resolving weaknesses in national security preparedness and communications; and privacy-based research that examines the responses of the public to the impact the proposed technologies will have on personal privacy. Although when drawn together these two perspectives create a relatively complete picture of their use, lacking are the motivations and public reactions to the technologies that have been adopted.

To understand the motivations of government and drivers for public motivation and adoption, Critical Social Theory (CST) developed by Jurgen Habermas[3] 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'.[4] CST's primary aim is emancipation through knowledge and study of past behaviour. 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 the popular media.

For future advancement of government-driven solutions to national security threats and preparations, it is imperative that current research looks beyond the solutions themselves and develop greater awareness of their implications. The outcome of this research is to provide a framework for evaluating the impact of location-based solutions to national security problems and not to limit the development of technology or to prevent its use.

2. Location-Based Services for National Security

Location-based services (LBS) exploit knowledge about where an information device is located. The information device can be used to locate living and non-living entities (people, artefacts in rooms, etc.). Location can be represented in a variety of ways, e.g. address or latitude/longitude. Depending on the context LBS can utilize several technologies for knowing where an information device is geographically located. Global positioning system (GPS), cell identification, broadband satellite network, assisted GPS, wireless local area networks (WLAN) and radio frequency identification (RFID) are examples of technologies used.[5]

LBS are used in multiple market segments: personal, commercial and government, for diverse purposes, including navigation and personalized marketing material dependent on location. LBS also provide a technological solution to the more serious issue of national security. Their ability to calculate position information (either push or pull in nature) provides an invaluable resource for preventive, protective and responsive situations. A pull technology requires the user to request the information, where a push service delivers the information automatically based on the position of the user. An example of the LBS technologies being used in national security include: RFID for disaster management, disease outbreaks, and secure access control; GPS devices for monitoring emergency response teams and the monitoring of public health outbreaks and mobile stations for emergency response.

3. Critical Social Theory in Information Systems Research

Qualitative research is used when the focus of research is the 'real world'.[6] The tools of qualitative research allow a researcher to interact with those that the

research phenomenon effects, both directly and through social artefacts like newspapers, popular magazines and other feedback sources.[7] A qualitative approach is most useful when a researcher wants to describe, interpret, verify or evaluate the impact of a particular area of interest.[8]

Critical Social Theory (CST) is a qualitative approach to research. There are three underlying paradigms in which qualitative research can take place: positivism, interpretivism and critical theory. Positivism and interpretivism are the two most common approaches used by researchers in Information Systems,[9] however over the past 20 years there has been a significant body of work that has been applying critical theory to Information Systems research topics.[10]

The critical approach differs from interpretivist in that it seeks to understand the workings of the whole phenomena: a critical study in Information Systems cannot look at technology alone, it must strive to understand it in terms of the industrial, societal and national context it is applied in.[11] It is the impact that innovation has had on the population that is most critical to its success or failure. A critical researcher aims to better understand how societies work to produce beneficial and detrimental effects, in this case through adoption of location applications. The researcher then looks for ways to mitigate or eliminate the damaging effects (of the location applications).[12] Critical researchers use knowledge that is grounded in social and political practices. Historical analysis of a phenomena is used to identify long-held associations.[13] McGrath[14] states that '[f]or more than 30 years, critical research in information systems (IS) has challenged the assumption that technology innovation is inherently desirable and hence to the benefit of all'. Cezec-Kemanovic,[15] Kirkpatrick,[16] Lyytinen and Klein,[17] Lyytenin and Ngwenyama,[18] Ngwenyama and Lee[19] and Wong[20] are researchers who have investigated and applied the work to IS research. It is a method designed to reveal 'hidden agendas, concealed inequalities and tacit manipulation' in the examination of the complex relationships of information systems, socio-political and organizational contexts.[21] CST is a qualitative approach to Information Systems (IS) research. It differs from an interpretivist perspective by its intention to emancipate the subjects of the study, rather than to empathize with them. Figure 1 describes the relationships between approaches to IS research and a suggestion of tools used to operationalize the theories.[22]

Where interpretive researchers seek to maintain the status quo,[23] critical researchers seek to emancipate subjects. Habermas's theory is intent on effecting radical change through understanding distortions of communications.[24] CST looks to the outside world and examines opinions that appear in the 'public sphere', defined by Fairclough as the connection between social systems and the domain of everyday living ('lifeworld'), where people deliberate on matters of social and political concerns.[25] Lifeworld is a term used by Habermas to refer to a common world of experience.[26] Cecez-Kecmanovic[27] describes it as the 'taken-for-granted universe of daily social activities of members'. CST implies that the researcher has an agenda and is setting out to examine the 'lifeworld' to come to understand the meaning of things.

Lyytinen and Klein[28] state: '[Habermas' critical theory] suggests that information systems which are designed to increase organisational effectiveness must also increase human understanding and emancipate people from undesirable social and physical constraints, distorted communication and misapplied power'. The questioning of the neutrality of technology is essential to understand the social impact of new schemes. Particularly in critical IS research, the aim is to expose

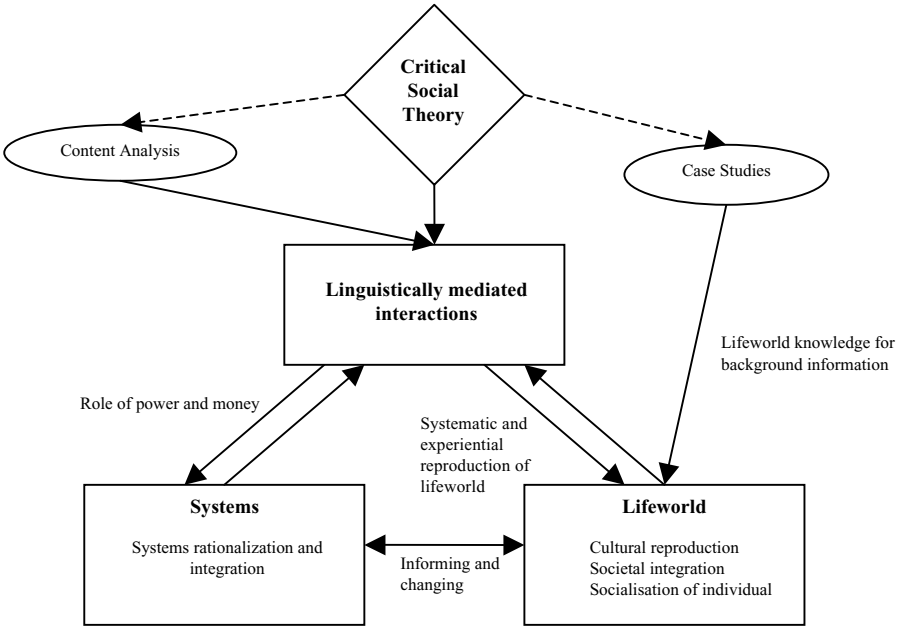

Figure 1. Methodological approach adapted from Titscher and Cecez-Kecmanovic.

attempts to 'design and (mis)use IS to deceive, manipulate, exploit, dominate and disempower people'.[29]

4. National Security and Critical Social Theory

The 'primary objective of CST is the improvement of the human condition'.[30] A number of technology studies have researched the importance of wireless services in disaster recovery efforts,[31] particularly the uptake of commercial network provision as a viable alternative for the small market of public safety. They have identified that if primary communications infrastructure is damaged or destroyed, it is the mobile services that are the lifeline. Connolly,[32] Chen[33] and Popp[34] identify the significance that IP location and Internet content can make in making knowledge links for counter-terrorism responses. In each of these studies, a particular application of the technology is examined, which allows for an in-depth understanding of the system to occur, but for disaster planning, it does not provide an over-arching view of the technology solutions being used together. Nor does it examine the impact these technologies can have when applied outside the realm of national security application.

Privacy studies have identified LBS technologies as being perceived as a threat to privacy regardless of purpose.[35] They have also examined the change in public perception to information collection and management for the purpose of 'homeland' security.[36] Halchin[37] 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 the counter argument to this is that by restricting access to online government information, potential terrorists are prevented from getting access, as are ordinary citizens.

Seifert[38] has written about the importance of information storage and collections in terms of infrastructure management, and related to this is the research by Raghu[39] that examines the need for collaborative decision making. This approach to national security research, although not from a technical or LBS perspective, is at least beginning to examine the problem holistically.

The use of CST will allow the researcher to investigate the impact that location applications for national security have through public perception. The content analysis tool Leximancer will be used to investigate the phenomenon through popular media sources. The content to be analysed can include words, phrases, sentences, paragraphs, pictures, symbols, or ideas.[40] Content analysis has gained momentum as a research method through the rapid expansion of mass communication, both mass media and international politics.[41] Content analysis is useful for making inferences by objectively and systematically recognizing particular patterns within messages and it does not need to be limited to textual analysis.[42]

Throughout this data collection and analysis, the researcher will be looking for indications of change in government perspective and response to events of interest, also for changes in public sentiment with regard to proposed solutions. Anecdotal evidence suggests that 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, e.g. event, time period, or technology, indicators of change will be able to be extracted and compared.

5. Conclusion

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 will be affected in order to enhance security cannot be denied. Previous studies have primarily focused on the implementation of a single LBS or the privacy impact of one location technology. From this it has been difficult to identify the continual shift in public perception and reaction to LBS. To determine the wide-ranging effects of the application of LBS to national security, the focus provided by CST, combined with the results of the content analysis, will bring together a detailed study of the concept of privacy and civil liberties being exchanged for security.

Notes and References

1. M. James, 'Where are you now? Location detection systems and personal privacy', *Science, Technology, Environment and Resources Section*, 2004.
2. I. K. Adusei, K. Kyamakya and F. Erbas, 'Location-based services: advances and challenges', *Canadian Conference on Electrical and Computer Engineering 2004 (IEEE Cat. No.04CH37513)*, IEEE, Vol.1, 2004, 1–7 vols.
3. J. Habermas, *Communication and the Evolution of Society/Jurgen Habermas*, translated and with an introduction by Thomas McCarthy, Heinemann, London, 1979; J. Habermas, *The Theory of Communicative Action*, Beacon Press, Boston, 1984.
4. H. K. Klein and M. Q. Huynh, 'The critical social theory of Jurgen Habermas and its implications for IS research', in J. Mingers and L. Willcocks (eds), *Social Theory and Philosophy for Information Systems*, John Wiley & Sons Ltd, West Sussex, England, 2004, pp. 157–237.

5. B. Rao and L. Minakakis, 'Evolution of mobile location-based services', *Communications of the ACM*, 46, 2003, pp. 61–5.
6. P. D. Leedy, *Practical Research: Planning and Design*, 8th edition, Prentice Hall, New Jersey, 2005.
7. *Ibid.*
8. *Ibid.*
9. W. J. Orlikowski and J. J. Baroudi, 'Studying information technology in organizations: research approaches and assumptions', *Information Systems Research*, 2, 1991, pp. 1–28.
10. D. Cecez-Kecmanovic, 'Doing critical IS research: the question of methodology', in E. Trauth (ed.), *Qualitative Research in Information Systems: Issues and Trends*, Idea Group Publishing, Hearshy, PA, 2001a, pp. 141–63; D. Cecez-Kecmanovic, M. Janson and A. Brown, 'The rationality framework for a critical study of information systems', *Journal of Information Technology*, 17, 2002, p. 215.
11. M. D. Myers, 'Qualitative research in information systems', *MIS Quarterly*, 21, 1997, p. 241; W. J. Orlikowski and J. J. Baroudi, 'Studying information technology in organizations: research approaches and assumptions', in M. D. Myers and D. Avison (eds), *Qualitative Research in Information Systems: A Reader*, SAGE Publications Ltd, London, 2002, pp. 51–78.
12. N. Fairclough, *Analysing Discourse: Textual Analysis for Social Research*, Routledge, London, 2003.
13. Orlikowski and Baroudi, 2002, *op. cit.*
14. K. McGrath, 'Doing critical research in information systems: a case of theory and practice not informing each other', *Information Systems Journal*, 15, 2005, pp. 85–101.
15. Cecez-Kecmanovic *et al.*, *op. cit.*; D. Cecez-Kecmanovic, 'Critical information systems research: a Habermasian approach', in *The 9th European Conference on Information Systems*, Bled, Slovenia, 2001b.
16. N. Lubick, 'Homeland security and geospatial data', *Geotimes*, 49, 2004, pp. 11–3.
17. K. Lyytinen and H. K. Klein, 'The critical theory of Jurgen Habermas as a basis for a theory of information systems', in E. Mumford (ed.), *Research Methods in Information Systems*, Elsevier Science Publishers, North-Holland, 1985, pp. 219–36.
18. K. J. Lyytinen and O. K. Ngwenyama, 'What does computer support for cooperative work mean? A structurational analysis of computer supported cooperative work', *Accounting, Management and Information Technologies*, 2, 1992, pp. 19–37.
19. O. K. Ngwenyama and A. S. Lee, 'Communication richness in electronic mail: critical social theory and the contextuality of meaning', *MIS Quarterly*, 21, 1997, p. 145.
20. C. K. Wong, 'Making sense of even a technology change: an interpretive approach to IT implementation', in R. H. Moorman and K. D. Kruse (eds), *Midwest Academy of Management*, Creighton University, Minneapolis, 2004.
21. Cecez-Kecmanovic, 2001a, *op. cit.*
22. See S. Titscher, M. Meyer, R. Wodak and E. Vetter, *Methods of Text and Discourse Analysis*, SAGE Publications, London, 2000; Cecez-Kecmanovic, 2001a, *op. cit.*
23. G. Walsham, 'Learning about being critical', *Information Systems Journal*, 15, 2005, pp. 111–7.
24. W. Cukier, R. Bauer and C. Middleton, 'Applying Habermas' validity claims as a standard for critical discourse analysis', in B. Kaplan, D. P. Truex III, D. Wastell, A. T. Wood-Harper and J. I. DeGross (eds), *Information Systems Research: Relevant Theory and Informed Practice*, Kluwer Academic Publishers, Massachusetts, 2004, pp. 233–58.
25. Fairclough, *op. cit.*
26. Habermas, 1984, *op. cit.*
27. Cecez-Kecmanovic, 2001a, *op. cit.*
28. Lyytinen and Klein, *op. cit.*
29. Cecez-Kecmanovic, 2001a, *op. cit.*
30. O. K. Ngwenyama, 'The critical social theory approach to information systems: problems and challenges', in H. E. Nissen, H. K. Klein and R. Hirschheim (eds), *Information Systems Research: Contemporary Approaches and Emergent Traditions*, North-Holland, Amsterdam, 1991.

31. K. Balachandran, K. C. Budka, T. L. Doumi and J. H. Kang, 'Third-generation wireless services for Homeland Security', *Bell Labs Technical Journal*, 9, 2004, pp. 5–21; B. L. Malone, 'Wireless search and rescue: concepts for improved capabilities', *Bell Labs Technical Journal*, 9, 2004, pp. 37–49.
32. G. Connolly, A. Sachenko and G. Markowsky, 'Distributed traceroute approach to geographically locating IP devices', in *Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 2003. Proceedings of the Second IEEE International Workshop*, 2003, pp. 128–31.
33. H. Chen, F.-Y. Wang and D. Zeng, 'Intelligence and security informatics for homeland security: information, communication, and transportation', *Intelligent Transportation Systems, IEEE Transactions*, 5, 2004, pp. 329–41.
34. R. Popp, T. Armour, T. Senator and K. Numrych, 'Countering terrorism through information technology', *Association for Computing Machinery. Communications of the ACM*, 47, 2004, p. 36.
35. L. S. Strickland 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*, 56, 2005, pp. 221–34.
36. L. E. Feinberg, 'FOIA, federal information policy, and information availability in a post-9/11 world', *Government Information Quarterly*, 21, 2004, pp. 439–60; B. N. Meeks, '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*, 46, 2003, pp. 15–6.
37. L. E. Halchin, 'Electronic government: government capability and terrorist resource', *Government Information Quarterly*, 21, 2004, pp. 406–19; L. E. Halchin, 'Electronic government in the age of terrorism', *Government Information Quarterly*, 19, 2002, pp. 243–54.
38. J. W. Seifert, 'The effects of September 11, 2001, terrorist attacks on public and private information infrastructures: a preliminary assessment of lessons learned', *Government Information Quarterly*, 19, 2002, pp. 225–42; J. W. Seifert and H. C. Relyea, 'Do you know where your information is in the homeland security era?', *Government Information Quarterly*, 21, 2004, pp. 399–405.
39. T. S. Raghu, R. Ramesh and A. B. Whinston, 'Addressing the homeland security problem: a collaborative decision-making framework', in *Intelligence and Security Informatics, Proceedings*, 2003, pp. 249–65.
40. T. O'Connor, *Research Methods*, 2004.
41. Titscher *et al.*, *op. cit.*
42. O. R. Holsti, *Content Analysis for the Social Sciences and Humanities/Ole R. Holsti*, Addison-Wesley, Reading, MA, 1969.