THE SOCIO-TECHNICAL SHAPING OF INNOVATION IN FACILITIES MANAGEMENT

Carmel Clifford-Lindkvist[1] and Abbas Elmualim

School of Construction Management and Engineering, University of Reading, Whiteknights, PO Box 219, Reading, RG6 6AW, UK

The introduction of Radio Frequency Identification (RFID) for security access control and workspace management was investigated through a case study in an organisation's Facility Management department. The use of RFID for security and for gathering information on how people use space in a building has some privacy implications. The aim of this paper is to examine the discourse of privacy discourse toward the technology in the organisation and explore how the issue of privacy and RFID is seen outside the organisation. The case study is explored through the use of ethnography, which involved semi-structured interviews; the collection of field notes and corporate artefacts. This approach insures a holistic exploration of how privacy impacts on the socio-technical development of the technology. The term "socio-technical" is developed by Bijker (1997) stating technical social and technology innovation emerge as two sides of the socio-technical coin during the construction processes of articles, facts and relevant social groups. Similarly, the application of RFID is socially shaped by the discourses external and internal to the organisation. There are three privacy discourses focused upon – employees; legislation and business and in order for the technology to be usable in the organisation a consensual discourse must be reached. It is this consensus that allows the project to continue in its' goal for using RFID for access control and creating an innovative method of examining workspace management.

Keywords: discourse, facility management, privacy, radio frequency identification (RFID), socio-technical.

INTRODUCTION

Everett Rogers (1983) states that, "an innovation is an idea, practice, or object that is perceived as new by an individual or unit of adoption" (Rogers, 1983:11). In this sense technology new to an organisation is innovative to that organisation. The technology of interest is Radio Frequency Identification (RFID) and the organisation that it is being introduced is a financial institute. The primary use of RFID in the organisation is security access control and examining innovative methods of using the data from system to feed into strategic and operational decisions within buildings. Clegg (1998) found organisations are the way they are largely because they are cultural objects, which are infused with value. The 'value' Clegg refers to come from the departments that make up an organisation. In organisations departments have an impact on the take up of new technologies. Rogers (1983) found that the rate of adoption of any innovation is in its suitability to fit in with the values, beliefs and past experiences of the social system it is being introduced. Rogers states, "the diffusion of innovations is often a social process, as well as a technical matter" (Rogers, 1983:4).

[1] c.m.clifford@reading.ac.uk

Clifford-Lindkvist, C and Elmualim, A (2008) The socio-technical shaping of innovation in facilities management. *In*: Dainty, A (Ed) *Procs 24th Annual ARCOM Conference*, 1-3 September 2008, Cardiff, UK, Association of Researchers in Construction Management, 637-645.

Technology development being both a social and technical process is often shaped by the discourses of individuals or groups within the society it is introduced. If these groups do not have a consensual discourse, conflict may emerge which result in delay's in it development and introduction. There are also external discourses out of the control of the society that also socially shape the technology. Henderson states that 'despite rhetoric to the contrary, design work does not flow in a neat linear pattern, but rather is beset, like those on the 'yellow brick road to Oz', with innumerable diversions, mishaps and patch-ups' (Henderson, 2007:9). These 'diversions, mishaps and patch-ups' must reach a consensus to enable the technology meet the needs of the organisation that it is being created in. As McLoughlin (2006) points out "the element which ultimately ties the network together and allows it to stabilise is the building of a 'machine'" (McLoughlin, 2006:96). The building of the machine or in the case of this paper the introduction of the technology is an indication that a consensual discourse has occurred amongst the different social groups.

Radio Frequency Identification (RFID) is a ubiquitous technology that is to use employee data for access control and workspace management in a financial institute. Privacy is an issue that impacts on the development of the technology for the organisation because it uses the information of employees in the organisation. Nissenbaum (2004) examines informational privacy in terms of contextual integrity, namely that determining threats needs to take into account the nature of a situation or context: what is appropriate in one context can be a violation of privacy in another (Nissenbaum, 2004: Alahuhta, 2005). The aims and objectives of the paper are to explore how the discourse of privacy socially shapes the technology use in terms of

- The organisations internal privacy discourse to RFID
- The organisation's employee discourse to RFID
- External privacy discourse to organisations wishing to use RFID

METHODOLOGICAL APPROACH TO CASE STUDY

The discourse of privacy toward the technology of RFID is examined in this paper through Critical Discourse Analysis (CDA). Chouliaraki and Fairclough (2002) examine discourse in positioned ways of representing other social practices as well as the material world, and reflexively representing this social practice, from particular positions in social practices. The term 'critical' implies making visible the interconnectedness between concepts and practices (Fairclough, 1995; Marston 2002). Chouliaraki and Fairclough (2002) examine CDA both as theory and method. For them, CDA theorises the mediation between the social and the linguistic – the order of discourse and the social structuring of semiotic hybridity or interdiscursivity. They see CDA as a method for analysing social practices with particular regard to their discourse moments within the linking of the theoretical and practical concerns (Chouliaraki and Fairclough, 2002). CDA works well with ethnographic research that locates discourse as a part of a wider set of social practices. Chouliaraki and Fairclough (2002) found that ethnography can benefit from CDA in the direction of reflexivity: data material should not be regarded as faithful descriptions of the external world but as themselves discursive formations that are assembled together to construct a particular perspective of the social world. CDA is a useful method of examining how discourse frames technology as it attempts to encapsulate what is being said in the context that it is being said.

The case study primarily used an ethnographic method over a period of two years. Ethnography methods allow for the study of people in their own time and sociology,

studying subjects in their "natural habitat" as opposed to the "unnatural" setting of the interview or laboratory" (Burawoy, 1991). The researcher was directly involved in the development and introduction of RFID into the organisation. This position allowed the researcher to become intricately involved in the project and develop an understanding of positions of participants in the study and to contextualise the data.

Data for this paper concentrates on an interview between the researcher and a Staff Union representative and a European Policy Outlook RFID 2007 working document – 'RFID: Towards an Internet of Things'. The focus of the interview was to gain an overview of employee's viewpoint of the technology and the process of its introduction. Other case study data in the form of field notes and corporate artefacts are also used to capture the essence of what was occurring in the organisation as well as key phrases and environmental descriptions. The European Policy document attempts to illustrate an external view of the technology. The European Policy document was chosen for analysis as it encapsulates a business/legislative view of RFID while also acknowledging the privacy issues.

BACKGROUND OF THE CASE STUDY ORGANISATION AND TECHNOLOGICAL DEVELOPMENT

The organisation is a leading UK financial institute and employs over 19,000 people in its UK administration centres and branches. It has its own Business Services Department (BSD) which is the facilities management group that manage services in administration centres and branches. The responsibilities of BSD range from strategic property solutions to the management and operation of the organisations' premises and facilities. BSD aspire 'to providing productive and motivating environments that support the business and the way people want to work' (Organisation's intranet, Business Services, 2006). Everyone who works at, or visits, this organisation is considered a customer of BSD.

The case study organisation follows the philosophy of enabling employees to have a work/life balance and therefore many of their employees are given the option to work flexible hours; which sometimes fall out of the 9 – 5 hours and Monday to Friday spectrum. They also have the option of working away from their desk and away from the office. This not only satisfies employees who prefer the flexibility of their work but also assists Facility Management in freeing space in buildings. Because employees have the option of working flexible hours, the organisation must also be flexible in its opening hours and services provided to employees/customers. Premises and facilities need to be available 24 hours a day, seven days a week, to suit the personal lifestyle choices of people as they balance their needs of work and home. (Field-notes)

The flexibility in working hours and the flexibility of working areas have created new challenges for the BSD in terms of not knowing how many people are using a building during various times in a day, week or month. The lack of knowledge of not knowing numbers in buildings results in Facility Managers basing some of their decisions on an intelligent guess. 'Managers of staff may know what their general pattern of behaviour are, but little direct thought is usually directed at understanding the way in which people use buildings, so their knowledge is often mythological, only approximating to the truth' (Eley and Marmot,1995:13). Finch (2004) claims that the continued use of informal evaluation techniques is likely to exacerbate the disparity between actual and expected performance. Finch (2004) outlines the difficulty faced by FM in the following;

> *"Occupancy patterns are becoming far less predictable with the demise of the 9-5 job and the advent of telecommuting. Innovative solutions need to be introduced to monitor occupant movement and to resolve peaks and troughs in space demand. Automatic identification, radio frequency tracking, machine vision and other IT devices may assist in collecting and interpreting such information". (Finch, 2004:54)*

The organisation is also in a position to replace their current security access control system in eleven of their administration buildings with a RFID enabled system. RFID works on a networked system; a RFID tag contains information, which can be read by a RFID reader and transported to a data base which can then make use of the information. The security of data depends on the class and generation of the RFID tag, they have the ability to be encrypted so that others with standard RFID readers cannot read the actual data on the tag (Sweeney; 2005). The case study organisation intends to place RFID encrypted tags into the identity cards of their employees. RFID readers would be positioned at entrances, secure areas and other key areas around the buildings. This ensures the security of the building but the system also has other benefits that are innovative to facility management. The innovative aspect of this case study occurs through the use of some of the data from the RFID system to feed into information for volume and capacity studies of buildings. The idea of using the RFID data in this way is innovative for FM as they will have strategic up to date data on all areas of buildings to feed into quick decisions on workspace and space management projects. This innovation is dependent on the installation of an RFID access control system and therefore the wider society needs must be considered in order for the innovation to take off. There are obvious clear business benefits for the organisation in having such a system as security would be updated and there is likely to be a more productive use of space in the building. However, there are privacy issues for using employee data from the system in this proposed way.

RFID AND PRIVACY ISSUE INTERNAL AND EXTERNAL TO THE ORGANISATION

RFID has been particularly contentious amongst privacy activist groups in terms of the capabilities of what the technology can do in reference to people's privacy. RFID is a technology that holds information and when this information is linked to a person, privacy issues come to the fore. As a ubiquitous technology, RFID is 'always on' 'anywhere/ anytime' and therefore expands the existing internet problem of online history into a comprehensive 'offline history'. Until now only a limited view of a person could be obtained by searching in data, a much more comprehensive picture can be painted of a person and his day to day behaviour in the ubiquitous vision (Mattern, 2005). Consumer and civil liberty groups are concerned about privacy issues of the use of RFID data particular in terms of;

- Use of the data by a third party
- An increase in targeted direct marketing
- The ability to track individuals
- The development of RFID without the involvement of consumers view
- The lack of knowledge the majority of consumers have about RFID.

(Parliamentary Office of Science and Technology, 2004 and Lace, 2005)

The European Policy Outlook RFID 2007 working document – 'RFID: Towards an Internet of Things' acknowledges the privacy concerns in relation to RFID but also

acknowledge the business benefits of RFID. The SWOT analysis below highlights the privacy/business dilemma with the use of RFID.

Table 1: European SWOT analysis for RFID

Strengths	***Weaknesses***
European RFID user sectors are open minded and represent global cutting edge technology applications (e.g. Metro, Tesco)	Many SMEs do not have sufficient equity capital to invest in RFID
Excellent research infrastructure and strategic projects	Patent situation in UHF
Strong industry with many SMEs all over Europe covering the full value chain	Differing awareness for technology potential and societal issues throughout Europe
	Insufficient harmonisation within Europe (different speed in taking up RFID)
	Lack of standard protocols
	Interoperatability issues between vendor products
	Still low degree of public procurement and government RFID application
Opportunities	***Threats***
High potential for efficiency gains in major sectors (e.g. consumer goods, trade, automotive, healthcare)	Strong competition from technology providers in US and Asia
Potential for job creation	Low-cost (dumping) overseas competitors
Important market share with the growing market for European technology providers (esp. RFID tags/readers, production equipment/machinery)	Highly fragmented competitive environment
	Speed of RFID application "roll-outs" in competitive markets such as Asia and US
	Short window of opportunity for market entry
Large potential for improved consumer service and the development of new markets	Lack of interoperability, different speed of implementation within the EU and with respect to major competitors like the US and Japan
Development of Privacy Enhancing Technologies (PET)	Absence of seamless value chains
Importance of a wide stakeholder dialogue has been realised, first experience already exist	Lack of consensus on societal issues and concerns

(European Policy Outlook RFID, 2007:8)

The opportunities include efficiency gains, job creation and improved consumer service while some of the weaknesses are differing awareness of the technology potential and lack of consensus on societal issues and concerns. Hence the SWOT analysis shows that yes there are business gains but the weaknesses and threats need to be addressed.

The case study organisation recognise the business benefits of using an RFID as a multiple application for firstly security access control and secondly workspace management providing data for volume and capacity studies. While recognising the business benefits, the organisation also recognised the privacy concerns. According to Mattern (2003), social and organisational effort will be required in order to prevent this brave new world of smart, interconnected objects becoming an Orwellian nightmare where Big Brother will be joined by lots of little brothers. Some employees expressed at various points in the project, often in a good-humoured manner 'I trust the company but I don't want to be tracked every time I go to the toilet!' (Various employees' views taken from field notes). Such comments while were said in light informal conversation had real meaning behind them, which was privacy is something that is personal and not organisational.

The organisation do not want an image of creating an Orwellian society or break down the relations that they have built up with employees and customers. The project team involved in developing the technology do not want to develop or be part of a big brother environment and wish to continue the open culture of the society while ensuring a secure building that can be used efficiently through improved workspace management methods. The project team developing the application of RFID sought a

way to reach a consensus to meet the needs of privacy of building users and the needs of the business. The application of using data for access control and space management involves the project team working with various departments within the organisation most notably the Staff Union. In a semi-structured interview, a union representative spoke about his view of the use of the organisation gathering information through the RFID system.

Union Rep: I don't have a problem with people gathering information – it is the use you make of it. …… Where we have concerns and where our members have concerns and where we have expressed those concerns and want to see procedures in place.... Em, again having that information isn't necessary a bad thing – it is the use you make of it - we want robust processes in place. Either you calculate that information in a way that isn't identifiable or you release that information in a way that isn't actually identifiable.

The Union Representative speaks for himself and represents the view shared by the staff union body and their members in this dialogue. The union representative recognised the organisational need for the RFID system and the staff union wished to work with the project to ensure that union members concerns were being met in the RFID project. The Union Representative own individual discourse towards RFID is that he doesn't have a 'problem with people gathering information – it is the use you make of it'. For the Union Representative it was the data generated from the RFID system that was the issue for privacy concern and not the system itself. He was of the view that the real issue was not RFID technology but data usage. The organisation also recognises that it is the application of this data enables security procedures and innovative methods in space management. According to the union representative, the overarching view for the staff union members were that 'robust processes' were going to be put in place for the usage RFID data. The Union representative is clearly open to the use of the data for the benefit of the organisation but the use of the data should meet data protection regulations.

The European Policy Outlook working document on RFID states in terms of Employee protection rights and RFID that "should the RFID application one day have a widespread effect on employee relations the resulting needs would be by no means novel or specific. RFID applications could simply be another justification for needs such as data protection and personal control over information, which are already known as an aspect of the everyday and widespread use of information technology in employment relations' (European Policy Outlook RFID, 2007:31). Therefore the use of RFID data would fall under the Data Protection Act 1998 and the organisation would have to comply with this act in order to use the data.

Over a period of one year, meetings were held between the project team, the staff union and other relevant departments to discuss the use of data for the RFID system. Discussions included the privacy concerns of employees; the current legislation on privacy and the use of data for security access control and workspace management. These discussions resulted in a consensual discourse that balanced privacy needs and business needs resulting in a written Code of Practice. The Code of Practice divides the data into 'static data' and 'operational data'. Static data will be used for security purposes and will include employee's personal details. A person in management can only access identification of an individual through the approval of a series of procedures and groups and must have good reason to access the information. The operational data will contain the tag number of individuals, times and locations of the

tags within the building. In this way the individual is not identified and can only be differentiated through their tag number. The owner of the tag number is anonymous. This code of practice of the use of the data satisfies the business needs and the employee concerns but also complies with the Data Protection Act 1998.

THE SOCIOTECHNICAL COIN AND REACHING A CONSENSUAL DISCOURSE

The above highlights the internal and external discourse of privacy toward RFID and how these impact upon the social/technological development of RFID into the organisation. The sociotechnical coin is a concept used by Bijker (1997) to describe how technology development and innovation is not purely a technical process but is also a social process. The above exploration of privacy discourse toward RFID supports Bijker (1997) argument that there is a social shaping of the technology and the technology shaping of society. There were three groups that were examined;

The employees who were concerned with how the organisation intended to use their data and the level this usage in terms of identifying individual employees;

The European document which focused on the general usage of RFID in organisations and complying with Data protection;

The project team wanted to use the technology for tracking people's movement to feed into security and space management but also wanted to comply with data protection and not compromise employee privacy.

It is these types of technology frames of shared assumptions, knowledge and expectations through which 'relevant groups' give meaning to an existing or emerging socio-technical configuration (McLoughlin, 2006). The perception of the technology as having a privacy issue was not unique to the organisation but was embedded in broader economic, political and social changes. The technological frame is not predefined but is developed throughout the process of developing the technology into the organisation. McLoughlin found that "the more developed a frame the more constraints are felt, the more closure in respect of openness to alternative interpretations and arguments exists, the more as a belief system it is stabilised, and the more 'hard' or 'obdurate' the socio-technical configurations which the frame gives rise to appear" (McLoughlin 2006:160). Reaching the stage of a developed technological frame within the organisation takes time. The relevant social groups in the organisation developing the technology frame must reach a consensus as to what they want that frame to be. It is the relevant social groups who will decide the frame for the technology that will suit the needs of the organisation and also meet external legislative obligations. As Gorse and Emmitt point out "whatever the legal constitution of the organisation there is a legal obligation for the business to comply with prevailing legislation, both UK, European and worldwide" (Emmitt and Gorse, 2003:91). The consensus was reached through discussions and cooperation of the staff union with the project team and written into a code of Practice. The technological frame for the RFID solution was based on the needs and wants of the organisation but also the discourses of the relevant social groups internal and external to the society. The organisation must comply with legislation and this therefore has an impact on how they use employee data.

CONCLUSION

The IST 2003 report of the European Commission found that instead of making people adapt to technology, we have to design technologies for people (European Commission, 2003). RFID, within the case study organisation, is being socially shaped by various social groups and shaped to meet the needs of the organisation. One of the needs for the technology to meet in is privacy concerns from employees within the organisation and legislative needs that come from outside the organisations control. The discourse of privacy is a prevalent issue for RFID technology and this issue must be addressed in order for the technology to be implemented. The Code of Practice drawn up for the use of the RFID data in the organisation attempts to meet these needs and documents a consensual discourse from the various groups involved in it's development. The Code of Practice draws up how the data will be used within the organisation that allows for the usage of data for security and volume and capacity studies while adhering to the Data Protection Act 1998.

Privacy as a discourse in the organisation had two sides within the organisation and an external side that came from legislative needs. McLoughlin (2006) sees how the different goals, values and tools for action that groups possess are derived from their technological frame. The RFID technological frame for the business offered benefits to security and space management but the RFID technological frame for NGSU brought on privacy concerns for data usage. Externally there were privacy issues and business benefits acknowledge through the EU paper but the paper sought out how meeting the privacy legislative should enable business and privacy issue reach consensus. In the organisation, once a consensus was reached to meet employee concerns and organisation usage of data, the technology can be developed and come closer to implementation in the organisation. The discourse of privacy external and internal to the organisation toward RFID highlights the socio-technical development of technology but also how reaching a consensus amongst discourses is important for the continued development of the technology.

REFERENCES

Alahuhta, P; Friedewald M; Gutwirth, S; Maghiros, I; Punie, Y; Schreurs, W; Verlinden, M; Vildjiounaite, E; Wrighe, D (2005) *Safeguard in the world of Ambient Intelligence (SWAMI): Scenario Analysis and Legal Framework: First Results*

Bijker, W (1997) *Of Bicycles, Bakelites, and Bulbs: Toward a Theory of Sociotechnical Change*. London: The MIT Press

Burawoy, M (1991) Chapter 1:Introduciton. *In:* Burawoy, M., Burton, A., Ferguson, A.A., Fox, K.J., Gamson, J, Gartrell, N., Hurst, L., Kurzman, C., Salzinger, L., Schiffman, J., Ui, S. (Eds) *Ethnography Unbound: Power and Resistance in the Modern Metropolis* Berkely, Los Angeles, London: University Of California Press

Chouliaraki, L and Fairclough, N (2002) *Discourse in Late Modernity*. Edinburgh: Edinburgh University Press

Clegg, S (1998) *Modern Organisations: Organisation Studies in the Postmodern World*. London: Sage

Eley, J and Marmot, A (1995) *Understanding Offices. What every manager needs to know about office buildings*. London: Penguin Books Ltd.

Emmitt, S and Gorse, C (2003) *Construction Communication*. Oxford: Blackwell Publishing

Fairclough, N (2005) *Peripheral Vision: Discourse Analysis in Organisational Studies: The case for Critical Realism*. London: Sage

Fairclough, N (1995) *Critical Discourse Analysis: The Critical Study of Language*. London: Sage

Finch, E (2004) Facilities management. *In:* D. Clements-Croome (Ed) *Intelligent buildings: design, management and operation*. London: Thomas Telford Limited

Gee, JP (1999) *An Introduction to Discourse Analysis: Theory and Method*. London and New York: Routledge

Gubrium, J and Holstein, J (2002) *Handbook interview research: Context and method*. London: Sage

Henderson, H (2007) Achieving legitimacy: visual discourses in engineering design and green building code development. *Building Research and Information* **35**(1), 6-17

Lace, S (2004) *Calling in the chips? Findings from the first summit exploring the future of RFID technology in retail*. National Consumer Council

Marston, G (2002) Critical Discourse Analysis and Policy Oriented Housing Research. *Housing, Theory and Society* **19**, 82-91

Mattern, F (2003) 'From Smart Devices to Smart Everyday Objects', Institute for Pervasive Computing, ETH Zurich http://www.grenoble-soc.com/proceedings03/Pdf/mattern.pdf

Mattern, F (2005) Ubiquitous Computing: Scenarios from an Informatised World. *In:* A. Zerdick, A. Picot, K. Schrape, J.C. Burgelman, R. Silverstone, V. Feldmann, C. Wernick and C. Wolff (Eds.) *E-Merging Media: Communication and the Media Economy of the Future* 145-163, ETH Zurich: Springer-Verlag,

McLoughlin, I (2006) *Creative Technological Change: The Shaping of Technology and Organisations*. London and New York: Routeledge

Nissenbaum, H (2004) Privacy as Contextual Integrity. *Washington Law Review* 79(1), 101-139

Pinch, TJ and Bijker, WB (1987) The social construction of facts and artefacts: or how the sociology of science and the sociology of technology might benefit each other. *In:* W.E. Bijker, T.P. Hughes and T.J. Pinch (Eds) *The Social Construction of Technological Systems: New Directions in the Sociology of History and Technology* London: MIT Press

Rogers, E (1983) *The Diffusion of Innovations* 3ed. New York: The Free Press

Sarantakos, S. (2005) *Social Research*. 3ed. New York: Palgrave MacMillan

Stringer, ET (1999) *Action Research Sage Publications*. London: Sage

Parliamentary Office of Science and Technology: Post note July 2004 Number 225: Radio Frequency Identification. (RFID)

European Policy Outlook RFID (draft version) Working document for the expert conference *RFID: Toward the Internet of Things* June 2007: Federal Ministry of Economics and Technology, Internal Case Study Organisational Documents.