Ethical Issues in Context Aware Ubiquitous Computing for Wireless Asset Management

Philip Davies[1], David Newell[1], Mak Sharma[2], Oliver Boothby[1]

[1]HCI Research Group, Faculty of Science and Technology,
Bournemouth University,
Fern Barrow
Poole, Dorset
daviesp@bournemouth.ac.uk
dnewell@bournemouth.ac.uk
i7954684@bournemouth.ac.uk

[2]Faculty of Computing, Engineering and the Built Environment,
Birmingham City University
Mak.Sharma@bcu.ac.ukroup

Abstract

In this paper we are concerned with the ethical implications of using Context aware RFID for Asset management. We consider work place use of RFID to manage assets and its impact upon staff privacy. We conduct surveys and interviews to determine staff views on closely monitored asset management. We discover that in the main staff are happy with this kind of monitoring of equipment using RFID systems. The conclusion shows that functional asset maintenance is feasible conceptually and ethically.

Keywords: RFID, privacy, asset management

1.0 Introduction

RFID was invented during the Second World War to identify military aircraft as friend or foe. This has developed considerably since then and RFID is employed in transportation, logistics, manufacturing, inventory control and animal tracking amongst other areas. A common used is tracking the movement of vehicles and is widely deployed in toll collection sectors. Ubiquitous asset management systems have been successfully implemented in manufacturing, logistics and traffic fields for many years. However in recent years, the price of Radio Frequency Identification (RFID) tags has dropped rapidly allowing RFID technologies to be employed more widely than previously and offering the potential for better use of staff time and enhanced cost savings. With the price of silicon decreasing in the past year [6] Corporate giants such as Tesco and Wal-Mart have been effectively

using RFID and EPC systems for years to enable better efficiency of logistics and allowing modelling of data in an ERP system, giving competitive edge. [16] With ever decreasing of cost RFID tags, this allows more innovation of RFID to be implemented in different sectors, as long as the value added outweighs the cost of the technology.

Tags are attached to an object which carries a small amount of data such as a manufacture or product ID. RFID networks allow the identification of a 'tag' using wireless electromagnetic fields. RFID has three main class types of tags; passive, semi-passive and active. Not all of these types of tag are suitable for asset management. Passive RFID is suited for inventory control and low-cost items due to the read range limit and active are more suited for High-cost items as the high range of communication gives a more accurate stand point. [13]. However, active tags are increasingly difficult to attach to mobile devices which make them unsuitable for a mobile asset management system. [17] Both Sanpechuda and Kovavisaruch and Wang argue that the type of RFID should be chosen around the application and purpose.

2.0 Ethical Problems

Due to the nature of RFID technology the network communicates wirelessly without notifying any parties that they or their equipment is being monitored and tracked. Consequently RFID tag usage has privacy issues associated with it. [6]. Garfinkel et al. [4] categorises two threats associated with the use of RFID tags: personal threats and corporate data threats. The primary concern of this study is the first of these and we will be looking exclusively at the personal threat arising from this the emerging technology.

Every RFID tag receives a unique shadow and thus is uniquely identifiable. This allows personal tracking since if a person is carrying an RFID tag they are traceable. Furthermore, since any RFID reader is able to gather information from tags, unauthorised parties could track any individual with a tag. [6] Now that readers are built into smartphones tracking could be implemented by almost anyone and be undetected. Garfinkel et al. [4] suggest that the benefits of RFID will be delayed if security and privacy issues are not correctly dealt with. These concerns are slowing down innovation and implementation of RFID and EPC systems in corporate and retail environments. Kelly and Erickson [7] talk of the individual's right "to be left alone" and suggest that tagging objects linked to an individual may be used to collect information about the individual as much as about the object and hence their daily life can come under scrutiny. The author puts forward hypothetical cases that raise potential legal issues. One instance asks the question if a burglary takes place through the third party tracking of an RFID on a high value item and the users/consumer gets assaulted, would the manufacturer who attached the tag be liable for damages. At the current time there is no legal answer to this hypothetical issue. [7]

3.0 Technical approaches

To meet some of these privacy issues a range of technical solutions have been suggested. One suggestion is that tags should be made responsive to "kill commands" to deactivate tags, block tags and rewrite the memory on tags. However this idea limits or completely removes the RFID purpose and would render the tag of limited usefulness. Another suggestion is that tag codes could be encrypted. This would give tags security, allowing privacy for users from unauthorised listeners accessing the tag data but would not stop the tracking of the tag by its RFID shadow. However the introduction of encryption raised the cost of the tags, something which manufacturers are trying to avoid. EPCglobal working closing with RFID manufactures to get tags to cost below five cents, this poses a conflict of interest between security and cost. [3]

Garfinkel et al. [5] and Kelly and Erickson [7] both agree that regulation is needed to solve the privacy issue before a restricting policy is put in place which could stop the technology from being taken up widely. However there is disagreement on whether it is ethical or unethical to collect information about the customer without their knowledge or agreement. Kelly and Erickson [7] suggest that as long as safeguards for data usage are in place to protect the customer, then it is acceptable to collect their information from RFID. However Garfinkel et al. [5] take the opposite view and suggest that the threat is unknown at present and further progress on implementation should be halted until legal legislation put in place. They suggest an "RFID Bill of Rights" [4] to bring fair practices to the use of RFID, giving five principles for deployment of low cost RFID systems. According to Garfinkle [4], users of RFID systems and purchasers of products containing RFID tags should have:

1. The right to know if a product contains an RFID tag.
2. The right to have embedded RFID tags removed, deactivated, or destroyed when a product is purchased.
3. The right to first class RFID alternatives: consumers should not lose other rights (e.g. the right to return a product or to travel on a particular road) if they decide to opt-out of RIFD or exercise an RFID tag's "kill" feature.
4. The right to know what information is stored inside their RFID tags. If this information is incorrect, there must be a means to correct or amend it.
5. The right to know when, where and why an RFID tag is being read.

We agree that there are clear ethical issues with RFID and it is important to make sure that all users/customers are aware of the system and its purpose as well as its implications for them personally.

4.0 Asset Management Problems

Into this ethical context many companies are looking for an automated solution for asset management and the targeted tracking of assets which is especially desirable for large companies. Businesses want to know which assets are leaving corporate buildings and when. Such a system allows the enforcement of resource policies more effectively. For example if a policy requires laptop user to be “off site at for at least 60% of company time” then it is difficult to manage this effectively without a great deal of manual input, time and effort. But using an RFID tracking system, the monitoring of all laptop movement could potentially be automated and data accumulated easily. However staff who carry their laptops from place to place are also tracked along with the laptop. Consequently there may be legal and ethical implications as well as policy implications that follow from the implementation of such systems.

In this paper we will look at the ethical implications from the point of view of staff whose movements around the workplace are being tracked. We look at staff sensitivity issues and whether there is likely to be staff resistance to the implementation of such a system.

5.0 Method

The approach was to gather information about staff sensitivity of RFID use from two data sources; one source was a questionnaire for general staff and the second interviews with IT specialists. The questionnaire was given to general workers in office environments to obtain their views on the tracking computer hardware. The second source was interviews with IT specialists to ensure the finished solution satisfied the demands of an enterprise environment.

A questionnaire was piloted with a focus group. One of the key aspects of the focus group was to check the English was not too technical and non-technical users could understand and complete the questionnaire. The feedback from the focus group was:

- some users did not see why the demographic questions were in place
- some did not know if they carried an RFID or NFC already.
- Some did not know what was meant by an RFID

As a consequence of the trial, text was added to the questionnaire before Question 3 to explain RFID.

The questionnaire was distributed online for a period of a week using non-age-specific channels on social media. The study was kept anonymous, and had a total of 41 responses.

6.0 Questionnaire Response

Two demographic questions were asked to see if there are any security and privacy concerns within different age groups and industries. All other questions were related to employee feelings on security and privacy concerns of NFC and RFID.

6.1 Demographic Results

The survey attracted replies from 15 industries with the top three bring IT, Health and joint third of Agriculture and Finance. Figure 1.

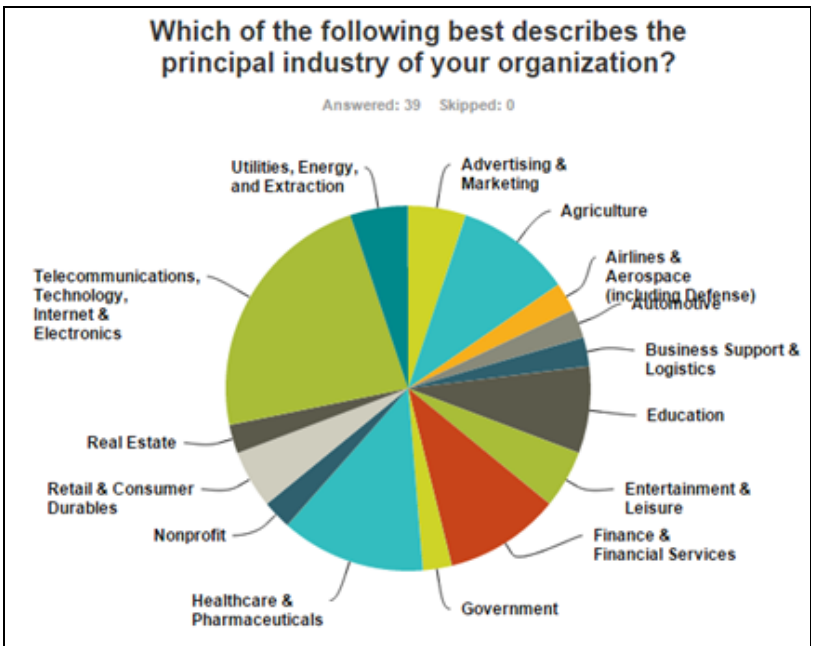

Figure 1: Industry Profile

Figure 2 shows that 76.90% of respondents were in the 18 to 44 age group with the sub age range of 18 to 24 having a minor majority, the remaining 23.10% being up to retirement age.

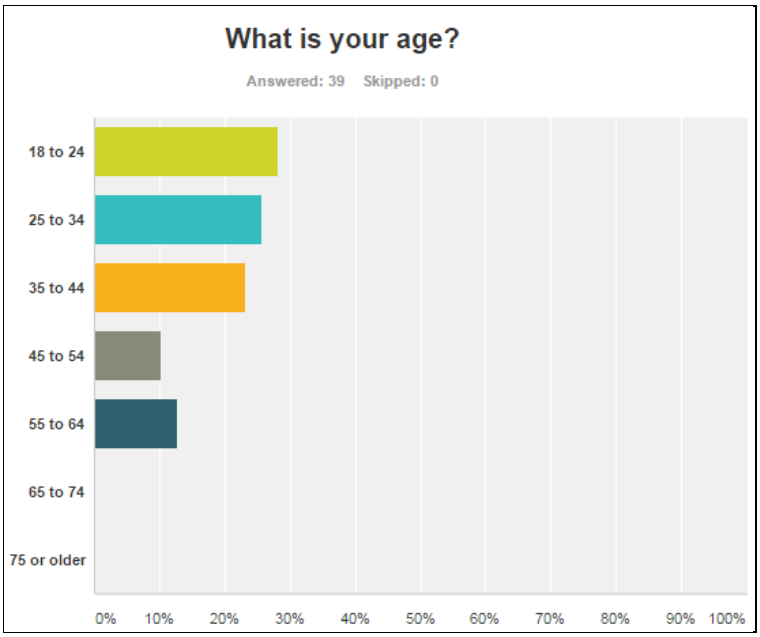

Figure 2: Age Profile

Largely the demographics of the respondents are broad in line with the diversity of both age and industry of employment.

6.2 Privacy Results

Respondents were asked about security and privacy of RFID, and questions related directly to their work environment.

First the question was asked if the respondents already carried an RFID or NFC tag and 64.10% acknowledge they already carry such technology.

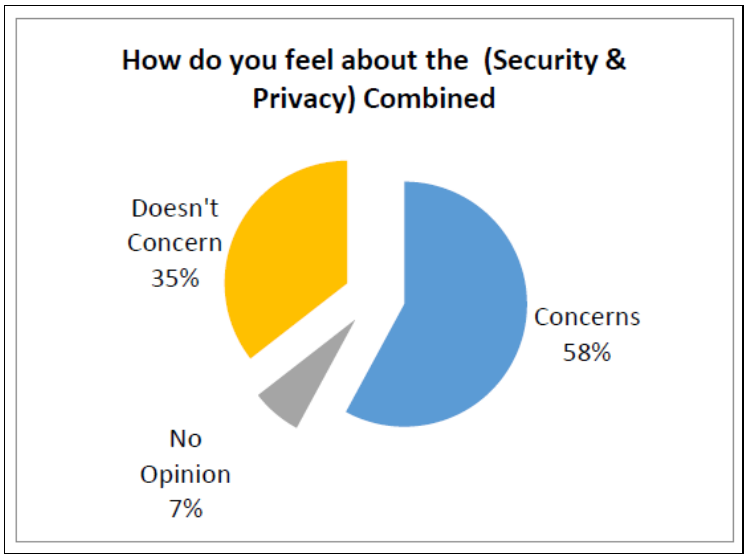

Figure 3: General Concerns about Privacy and Security

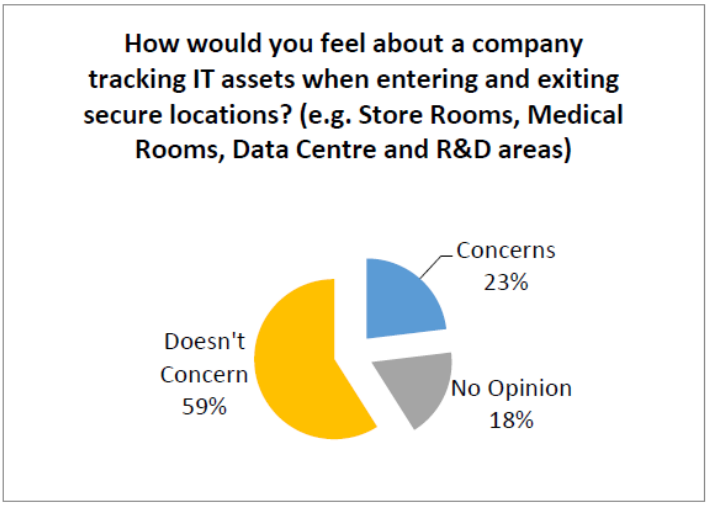

Figure 4: Concerns about Company Tracking

The respondents were then asked more directly about the issue of tracking in and around company buildings. The majority not having any concerns on both questions. Asked whether they had general concerns regarding privacy and security, 58% said that they did. Figure 3 In contract when asked if they had concerns about their company tracking them or their equipment only 23% said they had concerns, which is less than half. Figure 4 This suggests that most employers are trusted with tracking information.

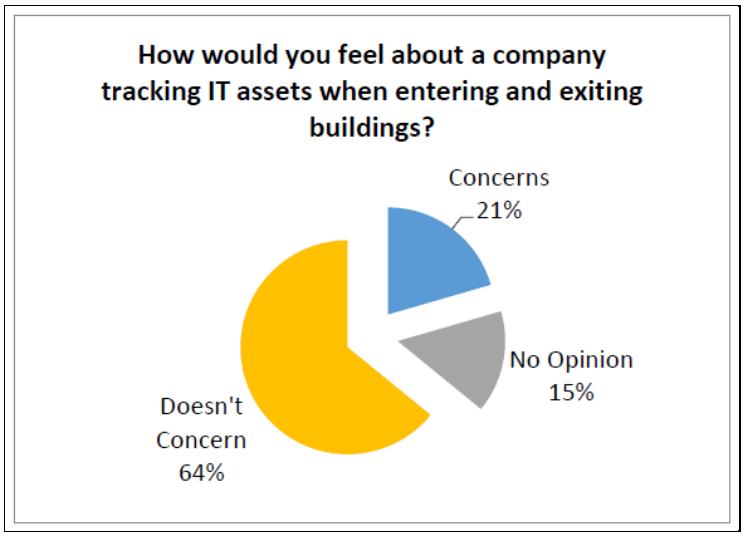

Figure 5: Entering and Exiting Buildings

Similarly there were limited concerns about the employer monitoring staff entering and exiting buildings with only 21% of staff showing some concern. This compares with 23% of staff concerned with the employer monitoring secure locations.

When asked if staff had concerns should their employer want to introduce and RFID tagging system, then 82.05% of respondents would not have an issue of an RFID system being implemented. Figure 6 This indicates that RFID technology is not subject to high levels of staff resistance and is likely to have a future in the workplace as part the of the internet of everything. The security and privacy of RFID are the main area of concern for respondents and this should be looked at in detail, with tracking being less of an issue.

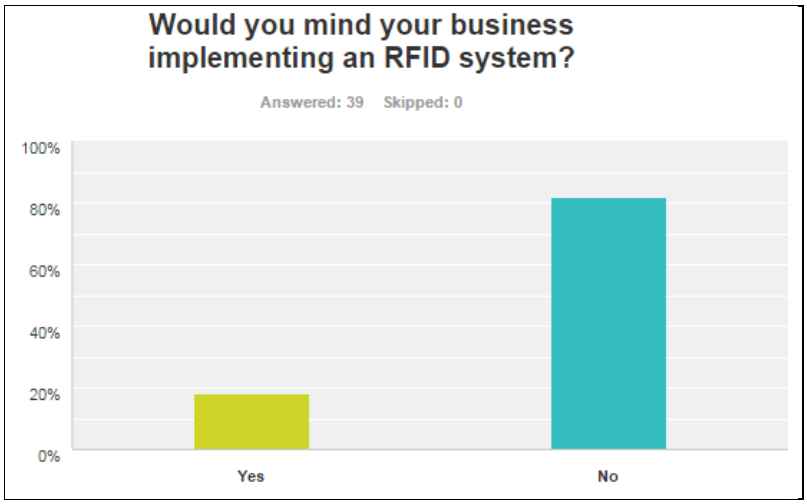

Figure 6: RFID Implementation

Of the respondents, 15% to 18% had no opinion on tracking, This may have been due to lack of information about RFID available or a lack of understanding about the implications for the responders

7.0 Conclusion

It is clear from this survey of general IT users that although the majority have concerns about privacy and security in a general IT context, this concern is reduced by approximately half when the issue concerns tracking by the person's own employer. This is an interesting result which may suggest that staff feel that employers can be more trusted than others when it comes to privacy and security information

The connection between employer and employee is already an intimate one as far as personal data is concerned. The employer already has a great deal of private information about the employee including personal address, health, ethnic and salary information. It might well be reasoned that information on movement is just a part of that overall package and so employers can be trusted with this additional data.

On the other hand it might be that employees feel that employers may have the right to this data if it concerns their equipment and their staff then they should know where they are located. Either way it suggests that companies which seek to implement the tracking of equipment and staff using RFID should have the larger part of the majority in their favour.

8.0 References

1. BBC, 2007. World's tiniest RFID tag unveiled. BBC Technology [online], 23 February 2007. Available from: http://news.bbc.co.uk/2/hi/technology/6389581.stm [Accessed 6 Mar 2015].
2. Dashevsky, V. and Sokolov, B., 2009. New concept of RFID reader networks structure: hardware and software architecture. 2009 International Conference on Ultra Modern Telecommunications & Workshops.
3. GS1, 2014. Regulatory status for using RFID in the EPC Gen 2 band (860 to 960 MHz) of the UHF spectrum [online]. Available from: http://www.gs1.org/docs/epc/UHF_Regulations.pdf.
4. Garfinkel, S., 2002. Adopting Fair Information Practices to Low Cost RFID Systems. Ubiquitous Computing 2002 Privacy Workshop [online]. Available from: http://simson.net/clips/academic/2002.Ubicomp_RFID.pdf.
5. Garfinkel, S. L., Juels, A., and Pappu, R., 2005. RFID Privacy: An Overview of Problems and Proposed Solutions. IEEE Security and Privacy Magazine, 3 (3), 34–43.
6. Juels, 2006. RFID security and privacy: a research survey. IEEE Journal on Selected Areas in Communications, 24 (2), 381–394.
7. Kelly, E. P. and Erickson, S. G., 2005. RFID tags: commercial applications v. privacy rights. Industrial Management & Data Systems, 105 (6), 703–713.
8. Khan, M., Sharma, M., and Prabhu, B., 2009. A Survey of RFID Tags. Int. J. of Recent Trends in Engineering and Technology, 1.
9. M Ayoub, K., Sharma, M., and Prabhu R, B., 2009. A Survey of RFID Tags. Int. J. of Recent Trends in Engineering and Technology, 1.
10. Motorola, 2015. RFID Asset Management Solutions - Motorola Solutions USA [online]. motorolasolutions.com. Available from: http://www.motorolasolutions.com/US-EN/Business%20Solutions/Product%20Solutions/RFID%20Asset%20Management%20Solutions_US-EN [Accessed 13 Mar 2015].
11. Oh, G., Kim, D., Kim, S., and Rhew, S., 2006. A Quality Evaluation Technique of RFID Middleware in Ubiquitous Computing. 2006 International Conference on Hybrid Information Technology.
12. Phillips, Karygiannis, and Huhn, 2005. Security Standards for the RFID Market. IEEE Security and Privacy Magazine, 3 (6), 85–89.
13. Sanpechuda, T. and Kovavisaruch, L., 2008. A review of RFID localization: Applications and techniques. 2008 5th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology.
14. TagCentric, 2015. Open Source RFID Edgeware [online]. TagCentric. Available from: http://tag-centric.sourceforge.net/ [Accessed 9 Apr 2015].
15. Transcends, 2015. Connecting the Internet of Things People (Web, Mobile, Social Media, Cloud) [online]. Transcends. Available from: http://www.transcends.co [Accessed 9 Apr 2015].
16. Violino, B., 2005. Leveraging the Internet of Things. RFID Journal.

17. Wang, B., Toobaei, M., Danskin, R., Ngarmnil, T., Pham, L., and Pham, H., 2013. Evaluation of RFID and Wi-Fi technologies for RTLS applications in healthcare centers,. Technology Management For Emerging Technologies.
18. Waspbarcode, 2015. Fixed Asset Tracking Software - Asset Management Systems [online]. www.waspbarcode.com. Available from: http://www.waspbarcode.com/asset-tracking [Accessed 5 Mar 2015].
19. Wu, D.-L., Ng, W. W. Y., Yeung, D. S., and Ding, H.-L., 2009. A brief survey on current RFID applications. 2009 International Conference on Machine Learning and Cybernetics.
20. Wyld, D., 2006. RFID 101: the next big thing for management. Management Research News, 29 (4), 154–173.
21. mobitec, 2008. RFID Middleware 1.0 [online]. MobiTec. Available from: http://mobitec.ie.cuhk.edu.hk/rfid/middleware/project.htm [Accessed 9 Apr 2015].