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.uk

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

using RFID and EPC systems for years to enable better efficiency of logistics and

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. Engineering 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 t-- 9 FreeF allI-7(D in,i)-1m(a)-v-8(m(a)-TJ 0 g(r)2(o)-12(m)25(a)-v-8(m di)7p)10(o

4.0 Asset Management Problems

Into this ethical context many companies are looking for 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 solutions 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

The questionnaire was distributed online for a period of a week using Google

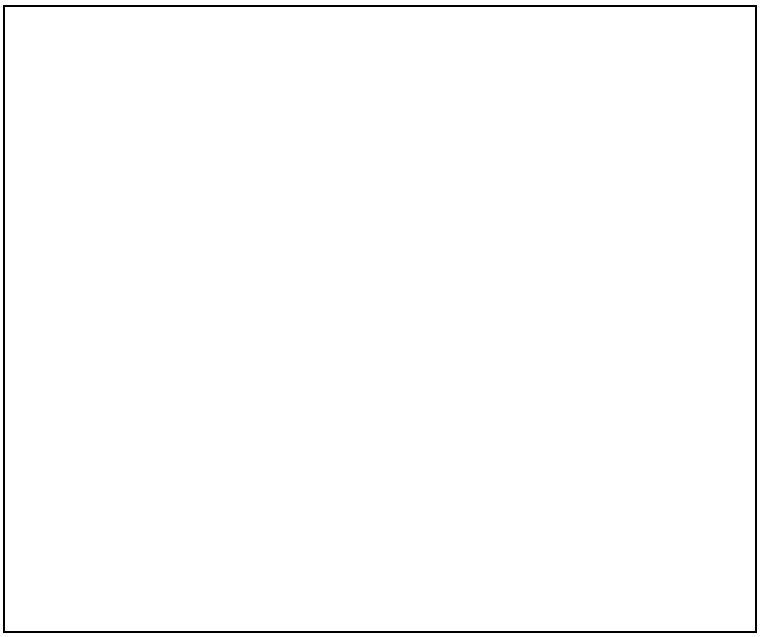

Figure 2 Age Profile

Largely the demographics of the respondents are b

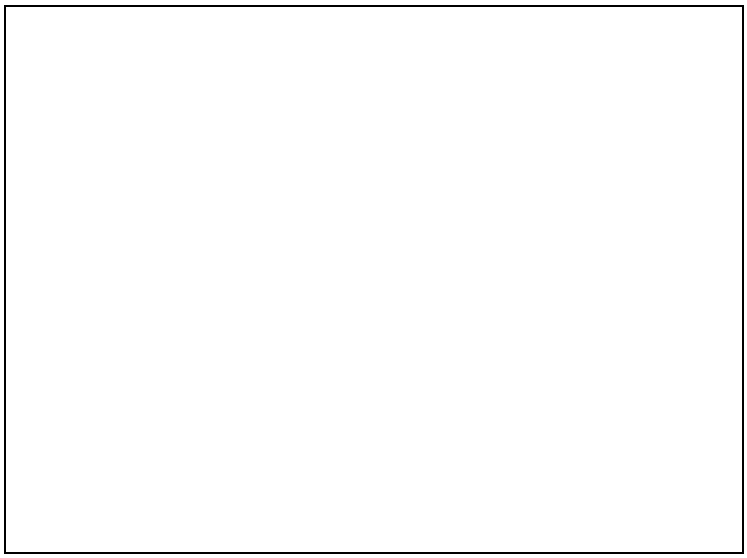

Figure 3 General Concerns about Privacy and Security

The respondents were then asked more directly about the use of tracking in and

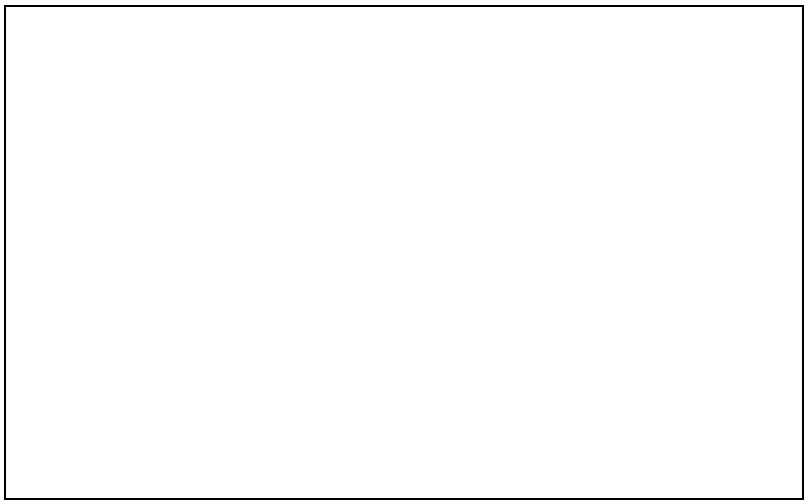

Figure 6 RFID Implementation

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 concedon006 Tc 2B0hc 20(n b)-12c 20(n)-7(n)5ee44b62(i)-17(5)1(e)-2w 7.663 0

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

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].