Security in Context: Investigating the Impact of context on Attitudes towards Biometric Technology

Chris Riley
NCR Global Solutions Ltd.
Swords, Co. Dublin, Ireland
cr230046@ncr.com

David Benyon
School of Computing
Edinburgh Napier University
d.benyon@napier.ac.uk

Graham I. Johnson
Advanced Technology & Research
NCR Labs, NCR Corp, Dundee.
graham.johnson@ncr.com

Kathy Buckner
School of Computing
Edinburgh Napier University

Biometric technologies are increasingly being used in a diverse range of contexts, from immigration control, to banking and personal computing. However, there has been little research that has investigated how biometrics are perceived across these different environments. This paper describes a qualitative investigation of the effect of context on attitudes towards biometric technology. Data collection was carried out in-situ in a train station, an airport and a retail environment. A categorisation of participants' attitudes towards biometrics is presented based on the data collected. There was little evidence for the perception of biometrics varying across the different locations, though security was found to be a more complex, context dependant notion that expected. The results are discussed with reference to notions of context and the acceptability of biometrics for future applications.

Context of Use, Biometrics, Acceptability, Privacy.

1. INTRODUCTION

Proving your identity has become a common occurrence in modern life. As information and communication technologies (ICT) become ever more pervasive we have to authenticate our identity at our place of work, when we make a purchase and when we travel. User authentication is a requirement of many computing systems but identity assurance is not a simple process. Traditional methods of user authentication, such as knowledge-based and token-based authentication, have a number of limitations. Passwords can be forgotten, copied or shared between users and physical identity devices or documents can be copied or stolen [24, 27] The high cost of password management in industry [19] and the possibility for PIN (personal identification number) observation during card transactions [29] are two obvious examples of the problems associated with existing user authentication.

An alternative approach to personal authentication makes use of users themselves. Biometric authentication is the process of establishing an individuals' identity through measurable characteristics of their behavior, physiology or anatomy. Biometric technology is no longer confined to research labs or sensitive locations and there are now many different commercially available systems. The attraction of using biometrics is that the characteristics used to authenticate identity cannot be lost, forgotten or readily stolen. A further, often cited benefit of biometrics is added convenience and the prospect of reducing 'password fatigue' [21].

There are numerous challengers associated with the introduction of any new technological system however, and biometrics pose a number of unique issues. Biometrics capture and store representations of one's 'self' and it has been argued that biometrics are an inherently emotive, ethically challenging technology [2]. Despite the reputed benefits, biometrics have not seen the level of uptake that many predicted [7] and the acceptability of biometric technology remains an open question.

This paper describes a qualitative investigation of peoples' perceptions of biometrics technology. The aims of the study were twofold. Firstly, we sought to understand what biometrics means to the people who would use them and build a rich picture of how the technology is perceived. Secondly, the impact of context of use on attitudes towards biometrics was assessed to determine how context affects peoples' opinions towards an emerging technology such as biometrics. The motivation for this work is described in below.

1.1 Biometric Authentication Technology

A review of the literature discussing biometrics reveals two distinct perspectives. There are those who describe biometrics as a positive development and many view biometrics as a new paradigm in user authentication that will eventually replace existing methods. For example Jain et al predict that given the benefits of biometrics the technology will eventually be used in almost every transaction requiring the authentication of identity [16]. However, biometrics are a controversial technology. Among

the criticisms leveled at biometrics are data security concerns [3, 20], loss of privacy [2] and the possibility of 'function creep' where biometric information is used in situations over and above what was initially agreed [8]. Until recently these issues were largely the subject of academic debate, but the United Kingdom's proposed Identity card scheme and recent high profile data security breaches have pushed these subjects on to a public stage [18].

The acceptability of biometrics will impact on the success of any implementation authentication systems. Firstly, the way biometrics are perceived will have an impact on the way they are used. People are generally considered the biggest variable in the performance of biometric systems [10] and the way the technology is perceived will affect system use. The connection between the perception of biometrics and usage behavior has lead some authors to propose that measures of 'user psychology' should be included alongside traditional metrics to describe biometric system performance [3]. Secondly, the way biometrics are perceived has clear ramifications for commercial services built around biometric authentication. There have been several cases of biometric systems being withdrawn or discontinued following negative feedback for users. For instance a biometric payment system was withdrawn from a US retail chain following a negative reaction from customers [26] and biometrics was withdrawn from Terminal 5 at Heathrow airport following complaints made to the Information Commissioner's Office. It could also be argued that deteriorating public opinion played a role in the scraping of the UK's ID card scheme. A number of recent studies have attempted to understand peoples' attitudes towards biometrics and this work is summarized in the following section.

1.2 Acceptability of Biometrics

Concerns about the privacy impact of biometrics is a theme that consistently emerges from empirical research on biometric technology. Coventry et al reported that privacy concerns emerged during focus group discussions about biometric technology [9]. A laboratory based usability evaluation found that participants were concerned about the privacy impact of fingerprint systems, which in turn had an effect on their confidence in the technology [31]. The popular perception of biometric technology was also investigated in the U.K. Passport Service biometrics enrolment trial. This is one of the largest published studies of biometric technology, with over 10 000 participants tested in multiple locations. The results indicate that most people were in favor of using some form of biometric technology in conjunction with national passports, although almost one quarter of participants were concerned about the effects of biometric technology on their civil liberties [32]. Privacy also emerged as a significant concern in recent cross-cultural survey investigating biometric technology [25]. Research to date suggests that people have conflicting, sometimes dichotomous views about biometric authentication.

1.3 Notions of Context

The acceptability of any product or interactive systems is inextricably tied up with notions of context [5, 22, 30] and technology that is appropriate for one environment or situation may be inappropriate in another. Given the emotive issues surrounding biometrics it is likely that context of use is particularly relevant. Context is a difficult concept to define and the term is used in different ways in the computing literature. Before discussing context and biometrics is worth reviewing how this concept is defined.

Much of the literature on context comes from the ubiquitous and mobile computing field and the idea of acquiring information about context or 'context-aware' computing looms large. Day et al [11] defined context as "…any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves."

Whilst this conception is useful from a context-aware or context sensing perspective, it is system centric and arguably too narrow to satisfy the wider HCI community. Ideas of context have changed as others have attempted to define what context means. Dourish advocates a broader model than encoding of contextual information but does not propose an explicit definition [12]. Others operationalize notions of context by discussing constructs such as the users' goals and characteristics, the tasks, the technical and physical environment and the social or organizational environment [22]. In the case biometrics all of these factors are relevant. It is reasonable to expect the environment of use to play a role in how biometrics are used and perceived. Queues, crows and authentication in public spaces are relevant as are organizational factors such as the institution offering the service, signage and branding. For these reasons the wider ideas of context, like those proposed in [22] will be used to inform this study.

1.4 Context and Biometrics

Anecdotal evidence for the importance of context can be seen in the relative success of biometrics in different applications. People have warmed to biometrics in certain applications, such as the use of biometrics personal and mobile computing devices. Though as discussed above, biometrics have been perceived less favorably in other contexts and this

has lead to the failure or withdrawal of a number of services built around biometric authentication.

There has only been a limited amount of research that touches on context of use and the acceptability of biometrics. One pan European study investigating how biometrics are perceived in air-travel environments found differences between participants ratings of biometrics across proposed contexts of use [6]. Air travel was rated as the most acceptable application for biometrics and authentication at public or government buildings was rated as least appropriate [6]. The authors concluded that biometrics are more acceptable in applications traditionally requiring a higher level of security. The only published study that was explicitly designed to investigate how context affects attitudes towards biometrics compared biometrics as used for personal and business transactions [15]. People were found to have more positive attitudes towards fingerprint systems when using the technology to complete a simulated personal transaction opposed to a simulated business transaction.

The rage of attitudes towards biometrics and the mixed fortunes of many commercial implications have lead us to question the role of context in the acceptability of biometrics. To investigate this issue a study was designed to assess how context of use influences attitudes towards biometrics.

2. METHODOLOGY

In most of the research described above, quantitative approaches have been used to investigate peoples' attitudes towards biometrics. Questionnaires have been the research instrument of choice across this work and few other methods have been adopted. Arguably, quantitative evaluation approaches are poorly suited to the investigation of nuanced issues like context of use [1]. People may not know how they would feel using biometrics in a particular context and the way someone may respond answering questions while seated at a computer is likely to be different to how they would react in a real world environment. The influence of environment, signage or crowding is difficult to capture using rigid data collection techniques such as questionnaires. Moreover, phenomena like privacy, acceptability or feelings of invasiveness are themselves not concepts easily reduced to numeric data [1]. We feel that a flexible research design is more appropriate when trying to disengage how context and environment of use affects peoples' attitudes towards biometrics. A qualitative study would represent a meaningful addition to the body of work on this topic.

For these reasons a flexible, interview based investigation approach was adopted during this study. A Grounded theory perspective was used to guide data collection and analysis. Grounded theory, originally proposed by Glaser and Strauss [14] has been used widely in the Human Computer Interaction and Information Systems domains [23]. One of the defining characteristics of grounded theory is the idea of allowing theories and themes to emerge from the data though a bottom up analysis process. A grounded approach was appealing as we sought to characterize and understand peoples' attitudes towards biometrics without predefining what we expected these concepts to be.

Although an a-priori perspective was carried into the evaluation though the investigation of different contexts of use, a grounded theory approach was felt to be the most appropriate for this study.

2.1 Study Locations

As this study sought to understand how context of use affects attitudes towards biometric systems the evaluation took place across several different locations. In situ data collection was seen as an important step in improving the validity this research. Interviews were conducted in an airport, a train station and a high street shopping environment. All three locations were in the United Kingdom. An international airport was chosen as a high security environment where people are familiar with visible security procedures. Train stations, though also within a transport context, have some obvious differences form airports. A retail context was chosen as the third location, as people are likely to have different goals and expectations in a retail space when compared to travel environments. Images from the three study locations can be seen in figure 1 below.

Figure 1. Images of the air travel, rail and high street environments where data collection took place.

Despite the differences between airports, train stations and retail spaces all three share a common need for identity management. There are

clear requirements to verify identity against travel documents in an airport and against payment systems (such as debit and credit cards) in both train stations and retail environments. Biometrics are beginning to be used in all three of these contexts and though most are small scale implementations or pilots, the proliferation of biometric technology across an increasingly diverse range of environments is likely to increase in the future.

2.2 Interviews

A semi-structured interview approach was adopted during data collection. Questions centered around peoples' perceptions of biometrics, addressing the subjective experience of using biometrics, problems or benefits arising from its use and perceptions towards security in general. The interviews tended to be brief, given the public setting and ad-hoc nature of the interviews, usually lasting less than five minutes. The interviews were recorded for later analysis and only limited notes were made during the interview process. Participants gave their consent to take part in study after introductions had been completed and a brief overview of the research had been given.

2.3 Usage Scenarios

Usage scenarios were also used during the data collect process. Previous research suggests that most people report a low level of knowledge of biometrics [6, 25]. This is a complicating factor when investigating attitudes towards biometrics as people may only have a limited understanding of the topic of interest. This raises the question of how to collect quality attitudinal information. For instance there is little point asking people to compare iris and vascular biometrics when they have not heard and do not know how such systems would be used.

The usage scenarios were developed as a way to mitigate these problems, providing a high level overview of how biometrics may be used in specific contexts. The scenarios were pictorial in nature, accompanied by a short description of the different applications. These scenarios were printed as postcards and were given to participants at the beginning of the interview.

The scenarios were carefully designed to reflect both the different contexts of use and the actual process of authentication. The scenario for the air travel context showed biometrics at an airline check-in kiosk. The rail travel scenario showed biometrics integrated into a ticketing machine as a payment enabler. The scenario for retail contexts also showed biometrics used as a payment enabler, integrated into a point of sale transaction. As this study was not designed to investigate perception of one particular technology, two versions of each scenario were produced depicting different biometric technologies. Fingerprint recognition was used as one example of biometrics as it's the most common and easily recognizable biometric. Facial recognition was used as a second biometric technology as this is a non-contact technology with different associations to fingerprint recognition. With two different technologies depicted in three contexts, a total of six scenarios were produced. Equal numbers of fingerprint and face recognition cards were used in each location. Each participant in this study saw only one usage scenario, corresponding to the environment where the interview took place.

The scenarios used during data collection in the air travel and rail environments can be seen in figure 2 below. The style and design of cards was similar across all three contexts.

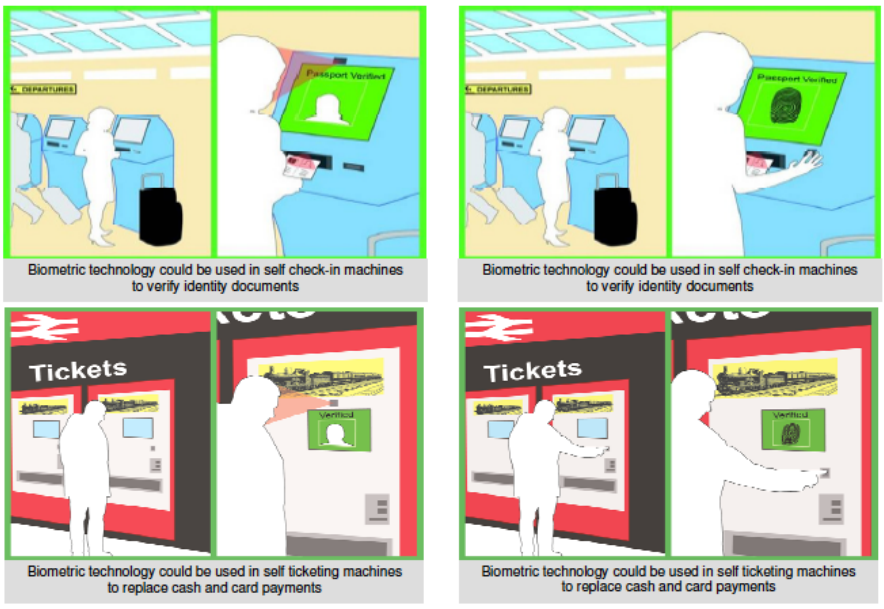

Figure 2. Usage scenarios depicting face and fingerprint recognition in air travel and rail contexts. Each participant received only one card.

2.4 Sampling Strategy

This study followed an opportunistic sampling approach. People were approached in each location and were asked if they wished to take part in the study. No attempt was made to select participants based on their age or gender. 20 interviews were carried out in each location with a total of 60 people taking part in this study. The majority of people who were approached agreed to take part in the research.

3. ANALYSIS AND RESULTS

3.1 Analysis process

Interviews were transcribed and the software package ATLAS.ti 5.5 [4] was used during data analysis. The analysis process followed an iterative coding process, where an open coding stage was followed by axial coding [28]. Through this process codes and comments coalesced into different themes which are presented below. Participants' attitudes towards biometrics are summarized followed by a comparison of responses across the different contexts.

3.2 Perceptions of Security

Security is a theme that participants in this study often made reference to. Security, in one form or another, was perceived as the main reason why biometric technology may be introduced across all three contexts. Notions of security were complex though, encompassing a number of constructs with different meanings to different people. For instance security meant a different thing in each context. In an airport environment biometrics and security was tied up with the ideas of physical security and counter terrorism initiatives. The scenario illustrated the possibility of biometric verification against identity documents (such as the biometric information contained in many modern passports) and this was interpreted by most people to be a security initiative rather than an efficiency or process improvement. In retail environments security tended to be related to payment security, fraud and identify theft. Participants' primary concern in this context related to the possibility of financial loss as opposed to personal safety. In a rail travel context perceptions of security were less clear, with ideas of security relating to physical security, ticket validation and payment security.

One of the more striking aspects of participants' perception of security was the dualistic nature of the concept. Almost everyone made reference to security vulnerabilities that may accompany the introduction of a new authentication system such as biometrics. People were aware that additional security features introduced corresponding 'attack vectors' which have the potential to compromise the security of the overall system. Comments such as the following were typical:

> "I think my biggest concern is once you put your fingerprint on it, could someone lift your fingerprint, just sprinkle some chalk over the back of it? My phone has one of these covers on it which your fingerprint sticks to…"

> "Well I guess I've have concerns about fraud with biometrics, all that sort of thing, because all these technologies at some point become vulnerable to fraud."

This awareness of security risks was common across all contexts and suggests that people have a more nuanced understanding of security than they are often given credit for in the literature on usable security. Although many other studies have documented people behaving in ways detrimental to security, such as choosing easily identifiable passwords [27], people in this study demonstrated a surprising awareness of how biometrics could be circumvented.

3.3 Attitudes Towards Biometrics

A number of other themes emerged from the interviews reflecting participants' attitudes towards biometrics. In all six themes were used to describe the range of views participants' expressed towards biometrics, with two positive dimensions and four negative themes emerging. The full list of themes identified is shown in table 1 below.

Positive dimensions	
Theme	Characterized by:
Convenience Factors	Belief that biometrics would be faster or more convenient than existing security/ authentication methods
Security Benefits	Belief that biometrics are more secure than existing alternatives or that additional security is beneficial
Negative dimensions	
Theme	Characterized by:
Reliability and Performance Concerns	Questions or concerns about the reliability or security of biometric technology when used in the 'real world'
Requirement for Biometrics	Questioning the need for biometrics or belief that existing authentication systems are adequate
Privacy and Ethical Concerns	Concerns about privacy, surveillance or function creep associated with the use of biometrics
Safety and Intrusiveness	Concerns about personal safety, hygiene or the level of intrusiveness using the technology would involve

Table 1. Dimensions of user opinion towards biometrics emerging from the interview data.

3.4 Positive Sentiments

Convenience factors were a seen as a positive aspect of biometrics and many people said they believed the technology would be easier or faster than traditional authentication systems. Many people also said that they would use biometrics if they made transactions more convenient. The following quote captures the sentiment many people expressed:

> "If was done correctly it [biometrics] could take a lot of hassle out of checking in and speed things up"

Convenience factors, along with additional security were the two main benefits people felt biometrics could offer.

3.5 Negative Sentiments

A number of negative themes also emerged from the data, with people expressing a range of concerns about biometrics. Doubts over the reliability or performance of the technology were perhaps the most commonly expressed concern. Phrases such as 'would it actually work?' were common and people often made reference to the potential for delays or added frustration.

Ethical and privacy issues were a second major concern that emerged. Fears of convert surveillance, privacy invasion were often referred to. For some people, there was a real fear of loss of privacy. Some stated that they would not use biometric technology in any situation where given the choice. Concerns over the involvement of the government or the police were also seen in participants' statements, even though the technology was portrayed in commercial contexts. The following statement reflects one participant's attitudes towards the technology:

> "...what information do they have and is it too much, because there is a whole lack of... everyone knows... everyone knows a little bit too much… a little bit big brother?"

More extreme views such as the following statement were also not un-common:

> "It's not natural, it's as though you are a criminal or something. That's [Biometrics] the first thing that happens if you go to court or something. Next you will have to give your DNA before you get your messages or something."

Even though most people expressed some concerns about biometrics, many participants would often go onto say they would still use the technology. This is in contrast to the strong reactions of a small number of participants who held very negative views of the technology. This later observation reinforces the notion that biometrics are a divisive technology and there are unresolved acceptability issues.

3.6 Context & Attitudes towards Biometrics

Responses were compared across the data collection locations and it became apparent that there was little difference in the way biometrics were perceived across the different contexts of use. There was little evidence that people felt differently about using biometrics in an airport, a train station or in a retail environment. Given the differences in the contexts and the proposed usage scenarios this was an unexpected finding. There was a trend of an increasing number of negative comments from an air travel, to a rail to a retail context, though it was felt this did not constitute strong evidence for a difference in participants' attitudes across contexts.

Individual differences, rather than differences arising from context, were much more apparent in participants' comments. The people who took part in this study often held very strong views about biometrics. Some held positive views towards the technology and others had a very negative perception of biometrics and unambiguously expressed this. A third group of people tended to have a more neutral view of biometrics, being largely ambivalent or expressing a lack of knowledge about biometrics or technology in general. There were people in all three environments who expressed each of these views. If context did influence attitudes towards biometrics this effect was not detectable in the polarized views many people expressed.

4. DISCUSSION

4.1 Contextual Effects

An aim of this study was to investigate contextual effects surrounding the acceptability of biometrics, though little evidence for this was seen. This was an unexpected finding as past research has suggested that context would affect the way biometrics are perceived. There are a number of interpretations for this result. It is possible that context does not have a significant effect on attitudes towards biometrics, though this seems unlikely given the body of literature concerning context and theories of technology acceptance in general. It could be that the different data collection locations were too similar for contextual effects to be seen. All three were public environments and if, for example, a train station had been contrasted with biometrics used in a home or educational environment effects of context may have been more apparent. The three settings share a public context, but it would be surprising if people felt there was no real difference between these environments.

It may have been the case that methodology employed was not sensitive enough to properly evaluate concepts like context and acceptability.

Given the flexibility of qualitative methods however, we feel this is unlikely to be the case. Qualitative, interview methodologies have successfully been used to evaluate a range of similar issues such as security in ubiquitous computing systems [13] and designing technology for religion [33]. In addition, the in-situ nature of data collection is likely to have made the methodology more sensitive to differences between the contexts. A further possible explanation is that people are unable to reliably describe their opinions towards a new technology like biometrics, without having used such systems. While this is an issue that affects all research on emerging technologies, other studies have found differences in peoples' attitudes towards biometrics, attributed to culture [6] and technology modality [25] with evaluation approaches that do not involve physical biometric systems.

A more probable explanation could be nature of participants' preconceptions towards biometrics. Biometrics are a unique class of technology which elicit strong views from many people. The media portrayal of the biometrics is also likely to have influenced peoples' opinions and people may have formed an impression of biometrics before ever encountering the technology. The polarization of peoples' views towards the technology makes it difficult to assess more subtle notions like as context or application. We believe that the more modest affect of context was over shadowed by the strong opinions people have towards
biometrics.

4.2 Methodology

Usage scenarios were employed in this study to ground discussions about biometrics in real world, commercial applications. Given the frequency that people asked questions about the scenarios and the references made, it was felt that these scenarios were a useful starting point for the data collection. There is a trade off though, between proving people with a clear scenario to comment on and influencing the results. The scenarios were designed to be neutral in tone but there is a risk that they could have biased the results or unduly influenced peoples' perceptions of the technology. For instance the similarly of the visual representations of biometrics could have contributed to the lack of difference seen between the contexts. However, given many participants' strong reactions towards the mention of biometrics it is felt that this is unlikely to have been the case. Overall it was felt that these cards were a useful addition to the data collection process.

4.3 Security as a Concept

Conversely security was a notion that was clearly tied up with context. Security meant different things in different environments and encompassed diverse concepts including counter terrorism initiatives, personal safety, fraud and identity theft. There was a range of attitudes towards the value of security too, from suspicion towards security measures to a resignation to ever increasing security in modern life. The dualistic nature of security was the only aspect expressed by a majority of participants. The participants who took part in this study demonstrated a surprising awareness of the risks associated with the introduction of a new authentication system and seemed to have largely pragmatic views about security.

4.4 Attitudes towards Biometrics

A range of attitudes towards biometrics were seen in this study. Privacy and surveillance emerged as concerns in this study, as reported in other research [6, 9, 25] but a willingness to use biometrics and convenience benefits also emerged as clear themes. Through the reductive process of data analysis some variation in the data was lost, however we feel the themes presented here offer a robust characterization of the range of opinions people hold. Four negative and two positive themes emerged from the data, but overall there were a similar number of positive and negative statements. Despite this equivalence, peoples' perceptions of biometrics were polarized. It was not uncommon for participants to express strong sentiment towards biometrics, particularly those who had a negative view of the technology. This supports the idea that biometrics are a contentions technology, which can illicit strong reactions. Regardless of the technology modality or the context of use, biometrics will likely remain unacceptable to a proportion of the population.

5. CONCLUSIONS

Understanding how new technology is perceived is not an easy task. The acceptability of biometrics is a subtle issue and there are many factors that are likely to influence peoples' attitudes towards the technology. This study failed to find any evidence for contextual effects influencing the acceptability of biometrics. This does not mean that context is unimportant or that the application will have no affect on how biometrics will be received. It is more likely that the strong views held by participants' in this study over shadowed any effect of context or installation environment. Media coverage of identification cards and public data breaches coupled with fictional depictions of biometrics mean that many people hold defined views towards biometrics before ever having used
them. The way biometrics are integrated into other applications will almost certainly affect the way people use the technology, but our data suggests that peoples' views towards biometrics as a class of

technology are more pronounced and obvious than any contextual effects.

These results also show that security is a complex, context dependant notion with significant scope for misinterpretation. Security was used as an umbrella term by participants and it encompassed a spectrum of different phenomena. The range of views identified re-affirms some of the challenges inherent in designing usable security systems. We are all accustomed to security warnings and reminders, but the disparate views on security seen here suggest that generalized security messages are likely to mean different things to different people. A system administrator's conception of 'security' and the system user's concept of security may be very different. Given the range of meaning attributed to security across contexts, a shared and unambiguous notion of security should be seen a pre-requisite for any usable security system.

Biometrics remain a controversial technology with a number of connotations. The need for more efficient and effective security process will increase in the future so biometric technology is unlikely to fall by the wayside. This research has implications for the way biometrics are evaluated and how such systems should be deployed. Our results also suggest that biometrics elicit strong views and the acceptability of biometric technology remains an issue. Innovative methods are required to better understand the fit between a technological system, context and user groups before more costly technology deployments are attempted. Biometrics are not appropriate for every scenario requiring personal authentication, but the discrimination between acceptable and unacceptable applications remains an open question.

6. ACKNOWLEDGEMENTS

We would like to thank both BAA and ScotRail for supporting this research and providing access to their facilities. We are also indebted to the Scottish Executive and Technology Strategy Board U.K. for their sponsorship of this project through the Knowledge Transfer Partnership scheme.

7. REFERENCES

[1] Adams, A., Lunt, P. & Cairns, P. (2008). A qualitative approach to HCI research. In P. Cairns & A. Cox, Research Methods for Human-Computer Interaction (pp. 138–157): Cambridge University Press.

[2] Alterman, A. (2003). "A piece of yourself": Ethical issues in biometric identification. Ethics and Information Technology, 5, 139-150.

[3] Ashbourn, J. (2000). Biometrics: Advanced Identity Management. Springer.

[4] ATLAS.ti (2009). ATLAS.ti Scientific Software Development GmbH. Version 5.5. http://www.atlasti.com/

[5] Benyon, D., Turner, P. & Turner, S. (2005). Designing Interactive Systems: Pearson Education.

[6] BioSec Consortium. (2004). Report on results of first phase usability testing and guidelines for developers.

[7] Celent Research. (2006). Biometric Technologies: Are We
There Yet? Boston.

[8] Chandra, A. & Calderon, T. (2005). Challenges and Constraints to the Diffusion of Biometrics in Information Systems. Communications of the ACM, 48(12), 101-106.

[9] Coventry, L., DeAngeli, A. & Johnson, G., I. (2003). Honest It's Me! Self Service Verification. Paper presented at the Proceedings of CHI 2003, Workshop on Human-Computer Interaction and Security Systems.

[10] Coventry, L., DeAngeli, A., & Johnson, G., I. (2003). Biometric Verification at a Self Service Interface. Paper presented at the British Ergonomics Society Annual Conference, Edinburgh.

[11] Dey, A. K., & Abowd, G. D. (2000). Towards a Better Understanding of Context and Context-Awareness. Paper presented at the CHI 2000 Workshop on the What, Who,
Where, When, and How of Context-Awareness.

[12] Dourish, P. (2004). What we talk about when we talk about context. Journal of Personal and Ubiquitous Computing, 8, 19-30.

[13] Dourish, P., Grinter, R. E., Delgado de la Flor, J. & Joseph, M. (2004). Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem Personal and Ubiquitous Computing, 8(6), 391-401.

[14] Glaser, B. & Strauss, A. (1967). The Discovery of Grounded Theory: Strategies for Qualitative Research Aldine Transaction.

[15] Heckle, R. R., Patrick, A. S. & Ozok, A. (2007). Perception and Acceptance of Fingerprint Biometric Technology. Paper presented at the Symposium on Usable Privacy and Security (SOUPS), Pittsburgh.

[16] Jain, A., Hong, L. & Pankanti, S. (2000). Biometric Identification. Communications of the ACM, 43(2), 91-98.

[17] James, T., Pirim, T., Boswell, K., Reithel, B. & Barkhi, R. (2006). Determining the Intention to Use Biometric Devices: An Application and Extension of the Technology Acceptance Model. Journal of Organizational and End User Computing, 18(3).

[18] Joinson, A. N., Paine, C., Buchanan, T. & Reips, U.-D. (2006). Watching me, watching you: Privacy attitudes and reactions to identity card implementation scenarios in the United Kingdom. Journal of Information Science 32(4), 334343.

[19] Jøsang, A., Zomai, M. A. & Suriadi, S. (2007). Usability and Privacy in Identity Management

Architectures. Paper presented at the Australasian Information Security Workshop: Privacy Enhancing Technologies (AISW), Ballarat, Australia.
[20] Langenderfer, J. & Linnhoff, S. (2005). The Emergence of Biometrics and Its Effect on Consumers. Journal of Consumer Affairs, Volume 39(2).
[21] Liu, S. & Silverman, M. (2001). A Practical Guide to Biometric Security Technology. IT Pro, 27-32.
[22] Maguire, M. (2001). Context of Use within usability activities. International Journal of Human-Computer Studies, 55(4), 453-483.
[23] Matavire, R. & Brown, I. (2008). Investigating the Use of "Grounded Theory" in Information Systems Research. Paper presented at the South African Institute of Computer Scientists and Information Technologists, Wilderness, South Africa.
[24] Renaud, K. (2005). Evaluating Authentication Mechanisms. In L. F. Cranor & S. Garfinkel, Security and Usability. O'Reilly.
[25] Riley, C., Buckner, K., Johnson, G., I. & Benyon, D. (2009). Culture & Biometrics: Regional differences in the perception of biometric authentication technology. AI & Society, 24, 295-306.
[26] Rothke, B., & Tomhave, B. (2008). The Biometric Devil's in the Details. Security Management.
[27] Sasse, A. (2004). Usability and trust in information systems. Cyber Trust & Crime Prevention Project.
[28] Strauss, A. C. & Corbin, J. (1990). Basics of Qualitative Research: Grounded Theory Procedures and Techniques: Sage
[29] Tari, F., Ozok, A. & Holden, S. H. (2006). A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passwords. Paper presented at the Symposium on Usable Privacy and Security (SOUPS), Pittsburgh, USA.
[30] Thomas, P., & Macredie, R. D. (2002). Introduction to the new usability. ACM Transactions on Computer-Human Interaction (TOCHI), 9(2), 69-73.
[31] Toledano, D. T., Pozo, R. F., Trapote, A. H., & Gomez, L. H. (2006). Usability evaluation of multi-modal biometric verification systems. Interacting with Computers, 18 11011122.
[32] UKPS. (2005). UK Passport Service Biometrics Enrolment Trial: Atos Origin. [33] Wyche, S. P., Aoki, P. M., & Grinter, R. E. (2008). Re-Placing Faith: Reconsidering the Secular-Religious Use Divide in the United States and Kenya. Paper presented at the Computer Human Interaction (CHI) Florence, Italy.